Présente :

Hackers : l'autre monde

la pertinence des moyens mis en oeuvre pour lutter contre la criminalité informatique en Belgique

Ecole des sciences criminologiques Léon Cornil
de l'Université Libre de Bruxelles
Directeur de mémoire : Monsieur Jean Spreutels

Philippe Delepeleere

licencié en criminologie

Année académique 2000-2001

Date de mise en ligne :20 janvier 2003

Résumé

La question principale de ce mémoire porte sur la pertinence des moyens mis en œuvre pour lutter contre la criminalité informatique.

La criminalité informatique est méconnue, peu ou pas définie, son étendue, ses causes ne sont pas clairement établies. Les raisons sont multiples, parmi lesquelles la plus présente est certainement la frilosité vis-à-vis des nouvelles technologies. Les personnes concernées n'ont pas de réelles connaissances de la criminalité informatique, soit car elles considèrent que celle-ci est trop « compliquée » et hésitent à donner des définitions, des solutions à un problème qui change de forme très rapidement, soit au contraire parce qu'elles la sous-estiment, phénomène classique dans les politiques de sécurité des entreprises.

Ensuite, il faut pointer l'importance des caractéristiques non pas du hacker, mais des hackers. Le piratage informatique, s'il peut être réalisé en groupe ou individuellement, trouve son origine dans les motivations des différents groupes de hackers à se dépasser mutuellement. Si au départ, le terme « hacker » ne désigne qu'un passionné d'informatique, il va prendre une connotation « criminelle » lorsque cette compétition entre groupes va amener certains d'entre eux à enfreindre la loi.

A cela, et c'est ici que la notion de groupes de hackers prend de l'importance, ils répondent qu'ils adhèrent à des lois autres que celles adoptées par la société. Ils établissent ainsi des codes, des règles de conduite, une histoire-même, remplie des faits et actes de pirates célèbres, créant ainsi une sous-culture hacker dans la culture dominante. A ce titre, les hackers sont pratiquement les seuls criminels à publier des écrits, des manifestes, à l'exception des groupes terroristes, expliquant leurs motivations ou leur mode de vie, de pensée.

L'apport de Sutherland et de Sellin est particulièrement intéressant, leur théorie sur la notion de groupe et de conflit de culture s'appliquant parfaitement aux hackers et à leur mode de fonctionnement.

L'étude de leur motivations a permis de souligner que si leurs actes pouvaient trouver leurs origines tant dans le plaisir simplement intellectuel tout autant que dans l'intérêt financier,

entre autres, le passage à l'acte était fortement dépendant de l'aspect de facilité présenté par la criminalité informatique.

Il est ainsi relativement simple de créer des dégâts de nature informatique, en surfant sur le Net, et ce, sans être un expert en informatique. Mais ceci ne fera pas de vous un hacker au sens strict…

L'aspect de facilité créera véritablement l'opportunité. Il faut préciser que le concept d'opportunité en matière de criminalité informatique est assez pernicieux car il fonctionne dans les deux sens : un système mal protégé peut autant être une cible potentielle qu'un système réputé inviolable. Tout dépendra du hacker.

Le concept d'opportunité amène à parler du troisième point le plus important de ce mémoire que ce sont les moyens de lutte mis en œuvre.

Il y a évidemment d'une part la prévention situationnelle, et d'autre part, la répression, traduite par la loi du 28 novembre 2000 relative à la criminalité informatique.

La prévention adoptée est principalement situationnelle. Cela s'explique pour deux raisons.

D'une part, en raison de la technicité sous-tendue par la criminalité informatique. Il est assez logique de recourir à ce type de prévention « moderne » face à une criminalité qui utilise également des moyens modernes.

Ensuite, ce type de prévention vise, notamment à réduire les opportunités, ce qui n'est pas nécessairement une bonne chose, mais certainement la plus logique et la plus vendeuse d'une point de vue économique.

Pour ma part, je pense que ce type de prévention est certainement la mieux adaptée, mais en aucun cas seule. Elle doit s'accompagner de toute une série de mesures « éducatives », de formation du personnel, des utilisateurs du réseau Internet,… Sans cela, les pirates auront toujours une longueur d'avance, en raison, entre autres, de l'utilisation intensive de l'ingénierie sociale.

En outre, pour rejoindre d'une certaine manière Durkheim lorsqu'il parlait de normalité et d'utilité du crime, la prévention situationnelle dans le domaine informatique a amorcé le développement de tout un secteur, composé des entreprises de sécurité informatique, de consultance, voire même de détectives privés informatique, si bien, qu'à l'heure actuelle, tant que des mesures complémentaires ne seront pas prises, le véritable bénéficiaire de la prévention situationnelle sera le secteur des entreprises de sécurité informatique.

L'intervention de l'Etat, limité à l'aspect répressif traduit d'ailleurs bien cette tendance. Se voyant dépassé par l'ingéniosité des hackers, celui-ci a abandonné la prévention au secteur privé, qui, il faut bien l'admettre, est certainement plus à même de remplir cette mission.

Mais, il me semble ici que l'Etat, plutôt que d'abandonner la prévention aurait dû d'une certaine manière délégué celle-ci, apportant tout le soutien nécessaire à une application efficace, dans le domaine de l'éducation ou de la prise de conscience des risques par exemple.

Ce n'est, pour l'instant, pas le cas, et il s'en tient à l'adoption d'une loi sur la criminalité informatique. D'emblée, quelques soient les qualités et défauts de cette loi, il faut souligner que ce type d'initiative démontre une nécessaire prise en compte de l'importance exponentielle prise par la criminalité informatique chaque année.

C'est d'ailleurs cette peur qui explique probablement certains débordements observés dans la nouvelle loi.

Cette peur se marque aussi dans l'absence de définition de concepts essentiels, avec en premier, la notion de criminalité informatique, ou encore de « système » ou de « données » informatiques.

Enfin, c'est également cette peur qui va lui faire justifier ces pratiques illégales, parfois de manière hasardeuse, sans tenir compte des reproches qui lui sont adressés.

La volonté de l'Etat, au travers de cette loi, est clairement d'avoir la main-mise sur le réseau Internet, principal vecteur de la criminalité informatique, « quelqu'en soit le prix » ou les moyens utilisés.

Hélas, cette volonté ne s'en tient qu'au discours, les moyens financiers et humains ne suivent pas le discours défendu.

Dès lors, pour reprendre notre question de départ, « les moyens mis en œuvre pour lutter contre la criminalité informatique sont-ils efficaces ? ».

Partiellement, ceux-ci étant pour l'instant plus réactifs, quand ont leur en donnent la possibilité, que préventifs.

Philippe DELEPELEERE

Mémoire présenté en vue de l'obtention
du grade de licencié en criminologie

HACKERS : L'AUTRE MONDE

De la pertinence des moyens mis en oeuvre pour lutter contre la criminalité informatique en Belgique

Directeur de mémoire
M. Jean SPREUTELS

Ecole des sciences criminologiques
Léon Cornil de l'Université Libre de Bruxelles

- Année académique 2001-2002 -

Ce mémoire est tout particulièrement dédié à ma maman et ma grand-mère qui m'ont soutenu et encouragé tout au long de mon parcours universitaire.

Ensuite je tiens à remercier Monsieur Jean-Pierre Spreutels pour avoir accepté de diriger ce mémoire et pour l'intérêt qu'il y aura porté.

De même, je remercie mes lecteurs, Claire Scohier et Cédric Strebelle pour leurs conseils avisés et souvent salvateurs.

Je remercie également mes amis pour leur aide et soutien de chaque instant, en particulier Gaëlle et Jean-Michel, sans qui ce mémoire n'aurait pas été possible.

Enfin, je remercie David pour ses conseils créatifs.

« Ne perdez jamais patience.

C'est souvent la dernière clé qui ouvre la porte… »

A. de Saint Exupery

Introduction

Notre société technologique contemporaine nous rend tous tributaires de l'informatique.

Quelques heures seulement après la naissance, le nouveau-né y est déjà confronté, dès l'instant où les données de son identité sont stockées dans les fichiers de l'état-civil.

Notre société actuelle connaît actuellement une *« seconde Révolution Industrielle »*[1].De nos jours, l'informatique est présente dans n'importe quel secteur d'activités, qu'il soit public ou privé.

Si son apparition nous a grandement simplifié la vie, elle nous a également apporté son lot de problèmes, inhérents à tout progrès. Désormais, tout est réglé par l'ordinateur : la sécurité, les transactions financières, l'administration,… Un simple « clic » maladroit peut entraîner un grand « couac ». Et quand ce « clic » est intentionnel, il devient criminel.

Dès lors, la question qui se pose est celles des garanties entourant l'usage de l'informatique, et plus précisément de son usage illicite, malveillant.

La question de la ***pertinence des moyens mis en œuvre pour lutter contre la criminalité informatique***[2] sera l'objet principal de notre exposé.

Pour répondre à cette question, nous allons successivement analyser les éléments-clés de la criminalité informatique[3] en général et des « hackers » en particulier, et voir, pour chacun d'entre eux, qu'elle est leur implication et leur rôle dans l'efficacité des moyens préventifs et répressifs mis en place.

---

[1] U., SIEBER, *La délinquance informatique*, Bruxelles, Story scientia, Précis et travaux de la Faculté de droit de Namur, n°9, 1990, p. 5

[2] Nous visons ici la criminalité informatique au sens strict, recouvrant les infractions spécifiques à l'informatique que sont le faux et l'usage de faux en informatique, la fraude en informatique, le hacking et le sabotage informatique.

[3] Les termes « criminalité informatique », « cybercriminalité », « cybercrime », crime informatique » seront considérés comme des synonymes dans cet exposé ; de même que les termes « pirate informatique », « hacker », « cybercriminel », « criminel informatique ».

Notre plan de travail sera le suivant.

Nous allons dans un premier temps aborder la criminalité informatique en général. Nous y développerons la notion de risque informatique, afin de voir le degré de prise de conscience du monde de l'entreprise, principale victime du piratage informatique, vis-à-vis de ce phénomène.

Ensuite, nous analyserons le réseau Internet, afin de souligner le rôle important qu'il va jouer dans la commission des infractions informatiques et le développement du hacking d'une manière générale.

Le point suivant sera consacré aux caractéristiques de la criminalité informatique, analysant les différentes définitions avancées pour ce concept, ainsi que les problèmes posés par son évaluation, tant « spatiale » que sur le plan financier.

Enfin, nous clôturons cette première partie par l'analyse succincte de la notion de respect de la vie privée et l'analyse du réseau Echelon

Dans la deuxième partie, nous nous intéresserons à ce qui constitue l'univers des hackers. Nous verrons que ceux-ci ont leurs propres règles, leurs propres cultures, leurs propres fondements idéologiques, si bien qu'ils forment un véritable monde à part.

Pour cela, nous commencerons par un historique du hacking, afin de pointer les éléments marquant ayant émaillé les trente dernières années en ce domaine.

Ensuite, nous analyserons les caractéristiques des hackers. Nous verrons quels sont leur langage, leur idéologie, leurs motivations ou encore leur conception du Bien et du Mal.

Nous terminerons cette partie par une présentation non exhaustive des principaux outils utilisés par les hackers pour commettre leurs infractions, que sont les virus et l'ingénierie sociale.

La troisième partie sera consacrée aux moyens préventifs visant à lutter à contre la criminalité informatique, et en particulier à la prévention situationnelle.

L'examen, conséquent, de la loi du 28 novembre 2000 relative à la criminalité informatique fera l'objet de la quatrième et dernière partie, que nous conclurons par une approche empirique de la Computer Crime Unit de Bruxelles, section spéciale de la police fédérale chargée des infractions informatiques.

Au terme de ces analyses, nous espérons être en mesure de répondre à notre question de départ et de confirmer ou d'infirmer notre hypothèse selon laquelle ***les moyens mis en œuvre pour lutter contre la criminalité informatique ne seront pas adaptés, en raison d'une part, d'un manque de connaissance précise et fiable du phénomène des pirates informatiques en particulier et de la criminalité informatique en général, et, d'autre part, du manque de moyens humains et matériels développés afin d'assurer l'efficacité d'une prévention et, en cas d'échec de celle-ci, d'une répression efficaces.***

Première Partie - La criminalité informatique

Tout d'abord, nous replacerons le risque informatique par rapport à l'ensemble des risques existants pour les systèmes et les données informatiques.

Nous centrerons principalement notre analyse sur la réaction et l'appréciation des risques par les entreprises, étant entendu que les diverses considérations qui seront faites sont applicables aux particuliers, mais dans des proportions évidemment moins importantes (quant au budget par exemple).

Ensuite, comment parler de criminalité informatique sans parler du réseau Internet ? Celui-ci a fait l'objet d'un développement exponentiel ces dernières années, faisant de lui un acteur incontournable de l'informatique en général, et de la criminalité informatique en particulier.
Nous verrons quelle est son importance, et partant, son influence sur le développement des pirates informatiques et de la criminalité informatique.

Ensuite, après avoir posé les bases que sont le risque informatique et le réseau Internet, nous nous intéresserons plus particulièrement aux caractéristiques de la criminalité informatique. Ce sera pour nous l'occasion de pointer que cette notion n'est pas aussi aisément définie qu'on pourrait le penser et que son étendue et son coût posent également des problèmes de détermination.

Enfin, nous terminerons cette partie par une analyse succincte d'un autre concept-clé, à savoir la notion de respect de la vie privée. Bien que celle-ci sera limitée à l'essentiel, étant donné qu'il ne s'agit pas d'une notion propre à la criminalité informatique, il nous paraît indispensable d'en parler de par sa violation systématique, concomitante à toute intrusion informatique.

Titre I – Le risque informatique et les autres risques

Grâce aux nouvelles technologies, le risque informatique est en pleine évolution.

Alors que les équipements encombrants ont fait place à des appareils miniaturisés, individualisés, mis en réseaux, les capacités de traitements, l'importance des stockages, se développent sans cesse, amplifiant et diversifiant la vulnérabilité des utilisateurs.

Dans certains secteurs, l'importance de l'informatique est telle, qu'une interruption prolongée se traduirait par une crise importante pour l'entreprise, largement dépendante de ses systèmes informatiques, et pour tout l'environnement qu'elle dessert ou dont elle bénéficie.

L'ensemble du matériel et des données informatiques est exposé à des menaces provenant de l'homme, de la nature, des moyens techniques, à travers les erreurs, les pannes, les accidents et les malveillances.

Voilà, en quelques mots, les différents éléments abordés dans cette partie, le but étant de pointer l'importance d'une protection efficace et adaptée, et ce, dans tous les domaines.

En effet, si une œuvre d'art devra être protégée de la détérioration et du vol, l'ordinateur devra également être protégé contre les malveillances propres à sa nature « informatique ». En plus d'être volées[4] ou détruites, les données informatiques peuvent être modifiées, copiées, détruites, sans qu'il soit nécessaire d'y avoir « physiquement » accès !

Au risque matériel, il faut désormais ajouter le risque immatériel.

Nous terminerons cette partie consacrée aux risques en soulignant la réaction des entreprises face à ces risques, ainsi que leur appréciation de ceux-ci.

[4] Nous visons ici le vol matériel.

Section 1 – L'accroissement des risques

Plusieurs éléments permettent de comprendre l'accroissement des risques encourus par les entreprises face à la délinquance informatique[5] :

• La décentralisation des systèmes :

L'utilisateur, ayant un accès plus aisé aux systèmes d'informations, joue un rôle de plus en plus important.

De plus, les changements technologiques modifient les attitudes des utilisateurs, sans que ceux-ci prennent nécessairement conscience des risques de malveillance et délit auxquels ils s'exposent.

Ainsi, plus le nombre d'ordinateurs se connectant à la société «mère » est important, plus les possibilités d'intrusion pour les pirates augmentent. Il est en effet plus simple de sécuriser un seul ordinateur que l'ensemble des ordinateurs qui lui sont connectés.

• L'interconnexion des systèmes :

Que ce soit au sein de l'entreprise (réseau local ou LAN[6]), au niveau national ou international (on y trouve des réseaux publics comme Internet ou des réseaux privés comme SWIFT qui est réservé aux banques), l'interconnexion des systèmes informatiques augmente les possibilités de transmission de fichiers dangereux comme les virus ou les trojans[7] et multiplie également les possibilités d'intrusion.

• L'explosion de la micro-informatique (dans les foyers et dans les entreprises) :

Plus qu'un choix, cette explosion constitue presque une nécessité actuellement afin de rester compétitif, rendant les entreprises dépendantes de leurs systèmes informatiques.

• Une transformation rapide des métiers liés à l'informatique :

La technicité croissante de certaines professions, par exemple dans le domaine de la gestion des banques de données ou des systèmes en réseaux, entraîne une certaine dépendance de l'entreprise vis-à-vis de ses informaticiens, renforcée par la mobilité et la pénurie de ceux-ci.

Ainsi, la vulnérabilité de l'entreprise s'accroît en raison de la valeur de l'information et de l'importance des flux financiers véhiculés, de l'utilisation de l'information comme valeur stratégique, et enfin en raison du décalage entre le rythme de l'innovation technologique et la diffusion des méthodes de prévention et de protection dans le domaine technique et juridique.

---

[5] P., ROSE, *La criminalité informatique*, Paris, Presses Universitaires de France, Coll. Que sais-je, 1995, p. 10.
[6] LAN est l'abréviation de Local Area Network.

Section 2 - Typologies des risques informatiques

De par la complexité même de l'informatisation de la société, il convient de parler non pas de risque informatique, mais des risques informatiques, ceux-ci menaçant la sécurité du système, du réseau, à tous les niveaux.

Les considérations suivantes sont valables tant pour le particulier que pour l'entreprise, mais c'est vis-à-vis de celle-ci que se centreront bien souvent les attaques (lorsqu'il s'agira d'actes criminels) ou que les dégâts seront les plus importants, les plus dommageables.

La sécurité d'un système d'informations s'analyse selon trois éléments[8] :

- *L'intégrité :* il s'agit de la propriété qui garantit la présence et la conservation sans altération d'une information ou d'un processus.

- *La pérennité :* qui concerne le maintien de cette intégrité dans le temps ; elle nécessite que les informations soient accessibles aux personnes autorisées lorsqu'elles en ont besoin.

- *La confidentialité :* qui assure que seuls les utilisateurs habilités ont accès aux informations.

Cette trilogie « intégrité – pérennité - confidentialité » détermine la valeur de l'information.

Ces informations sont exposées à différents risques, qui peuvent être accidentels ou naturels. Il existe plusieurs classifications des risques informatiques, comme celles opérées par le CLUSIF[9], dont voici le schéma.

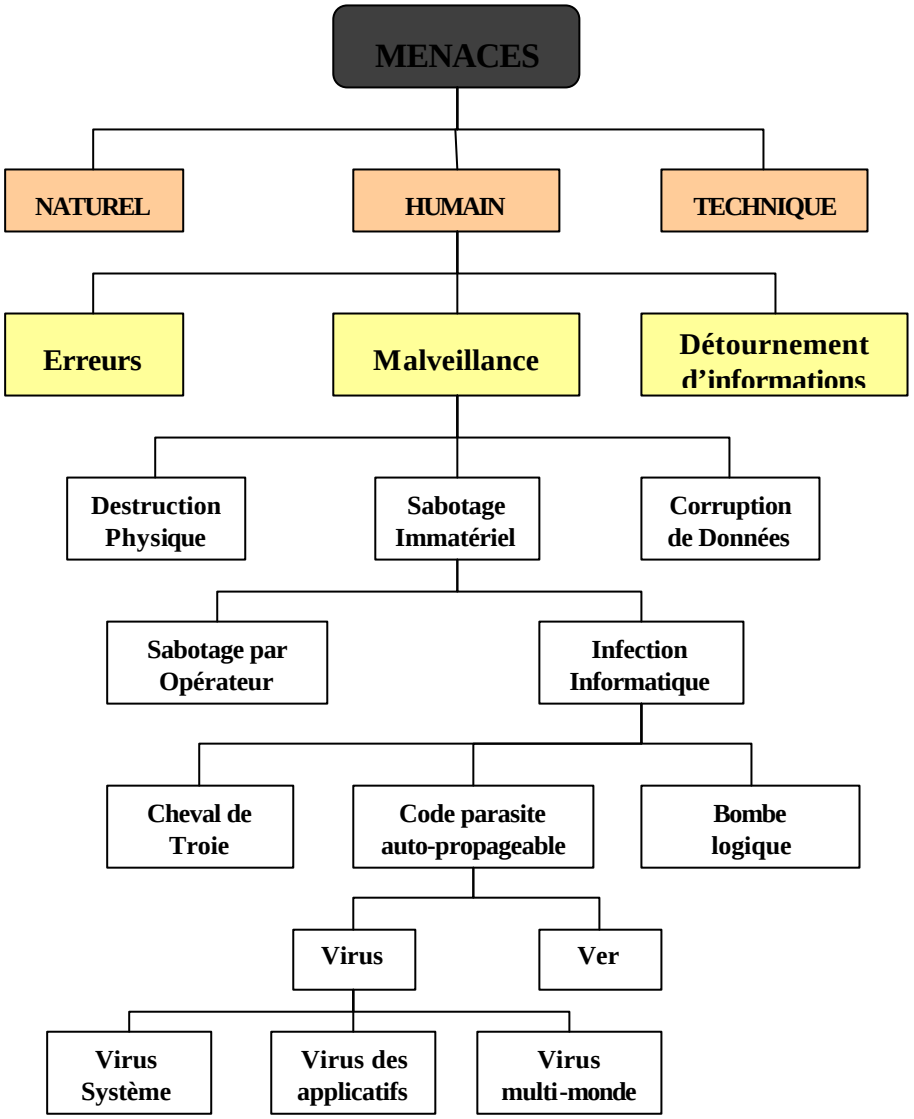
---

[7] Nous les analyserons plus tard.

[8] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 9.

[9] Il s'agit du Club de la Sécurité des Systèmes d'Information Français, qui regroupe 200 sociétés et organismes désireux de faire progresser la sécurité informatique.

Classification du CLUSIF



Le sujet de ce mémoire étant le piratage informatique, il ne nous semble pas indispensable de nous étendre sur ces différentes classifications ou leurs justifications.

Néanmoins, le hacking[10] constituant un risque en soi, un rapide survol de la question n'est pas inutile.

[10] Le hacking, tout au long de cet exposé , ne désignera pas uniquement l'infraction visée par la nouvelle loi du 28 novembre relative à la criminalité informatique, mais l'ensemble des infractions commises par les pirates informatiques, les « hackers ».

Il existe principalement trois catégories de risques : les risques naturels, les risques techniques et les risques inhérents au facteur humain.

A. LES RISQUES NATURELS

Ce type de risques est souvent considéré comme rare et donc peu pris en compte lors de l'installation des sites accueillant les systèmes d'informations.

Pourtant, il conviendra de choisir des lieux pouvant se prémunir contre les inondations, les tremblements de terre ou encore les chutes de foudre.

En effet, la foudre peut faire fondre les circuits imprimés en provoquant une surchauffe du système (entre autres), l'eau peut définitivement endommager le système en provoquant un court-circuit,…

Si ces risques semblent exceptionnels, ils n'en sont pas moins réels.

Ainsi, lors de l'été 2000, un violent orage s'est abattu sur Ottawa, inondant plusieurs sous-sols dont ceux d'une société d'entretien de systèmes. Les dégâts, chiffrés en centaines de milliers de dollars, n'étaient pas couverts par l'assurance, ces risques n'ayant pas été pris en compte. De par l'activité de la société, les dommages affectèrent non seulement le matériel de la société, mais également de nombreux utilisateurs. Et comme aucune mesure d'urgence n'avait été prévue, les activités de la firme n'ont pu reprendre que trois mois après l'incident[11].

B. LES RISQUES TECHNIQUES

Ces risques touchent surtout le fonctionnement proprement dit des moyens matériels et concernent la climatisation, l'alimentation électrique, le back-up, les incendies,…

Le fait que ces éléments constituent à proprement parler des risques n'est pas à nier aux vues des dégâts qu'ils peuvent occasionner, même si des solutions techniques sont, la plupart du temps, facilement envisageables.

Ainsi, une explosion à l'usine de production électrique desservant le quartier de Manhattan en septembre 1999 provoqua une série d'incidents au sein de diverses bases de données parmi lesquelles celles du New York Exchange où la fermeture prématurée entraîna la perte d'un nombre important de transactions.

Selon l'APSAD[12], 60% des PME et PMI [13] victimes d'un sinistre informatique majeur disparaissent dans les cinq ans.

---

[11] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 9.

[12] Il s'agit de l'Assemblée plénière des sociétés d'assurances et dommages.

[13] Ces sigles représentent respectivement les petites et moyennes entreprises et les petites et moyennes industries.

Les entreprises reconnaissent d'ailleurs volontiers qu'elles ne peuvent plus se passer de leur informatique :

- 40% ne peuvent fonctionner sans ordinateur plus de 4 heures
- 10% plus d'un jour
- 20% plus de trois jours
- 30% plus d'une semaine

Mais, paradoxalement, on constate que la protection des informations est moyenne dans 70% des cas[14].

C. LE FACTEUR HUMAIN

Tout comme les risques naturels et techniques, les erreurs de programmation, les négligences, … peuvent également avoir des conséquences très lourdes.

Au mois d'août 1999, à Suitland dans le Maryland, un ouvrier a ainsi déclenché le système d'arrosage sprinkler protégeant les ordinateurs du Bureau de recensement contre l'incendie. La salle des machines s'est d'abord vue inondée, avant de faire l'objet de plusieurs courts-circuits lorsque l'alimentation de secours s'est déclenchée ![15]

La grève et le départ de personnel stratégique constituent également des risques humains à prendre en compte. Sans être un acte criminel, une grève peut néanmoins paralyser les activités d'une entreprise, tout comme le départ d'informaticiens ou de techniciens spécialisés.

La notion de crime ou délit suppose un élément moral, c'est à dire l'implication humaine par une action volontaire ou non.

Les actions volontaires peuvent toucher le matériel, les informations qui y sont stockées, les réseaux,… Elles se traduisent par des destructions physiques, du sabotage matériel et immatériel ou encore le vol ou la corruption de données[16].

C'est bien évidemment dans la catégorie des risques liés aux facteurs humains qu'il nous faut placer le risque que constitue la criminalité informatique.

---

[14] Ces chiffres, donnés à titre indicatif, concernent la France, mais de par les similitudes avec notre pays, notamment sur les plans géographiques, technologiques,… ils peuvent nous donner une idée de la situation belge.

[15] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 11.

[16] Nous reviendrons ultérieurement sur les différents types de crimes informatiques.

D. CONCLUSION

A titre de conclusion, nous tenions à pointer un fait marquant relevé par une étude[17] portant sur la sinistralité en France[18] menée par le CLUSIF en 2000[19].

Nous y apprenons tout d'abord que les éléments relevés dans l'analyse qui précède, n'ont, apparemment, aucune incidence sur la politique de sécurité des entreprises, celles-ci continuant à se croire invulnérables. Il s'agit là d'une attitude de négligence extrêmement dommageable et très répandue. Ainsi, les entreprises se pensent à l'abri des risques naturels, comme les inondations, les tremblements de terre, les incendies,…, à l'abri des risques techniques, comme les pannes d'électricité, les surcharges de courant,… ainsi, et c'est bien le plus grave, qu'à l'abri de l'erreur humaine.

Comment expliquer cette attitude ?

Tout d'abord, il y a le fait que certaines entreprises rechignent à avouer qu'elles ont été victimes d'actes de criminalité informatique pour éviter une perte de crédibilité, et donc d'investissement de confiance de la part de leurs investisseurs et clients. Cette pratique aura pour conséquence que d'autres entreprises ne seront pas nécessairement conscientes des risques qu'elles courent et auront probablement tendance à les minimiser.

Ensuite, une piste de réponse doit être trouvée dans l'idée que ces entreprises étant, ou s'estimant, toutes puissantes sur le domaine économique, elles pensent sans doute étendre cette domination au domaine de la sécurité. Mais cette explication ne s'appliquant pas aux PME, aux petites entreprises familiales, …, un deuxième élément de réponse doit vraisemblablement être abordé : celui du budget alloué à la protection de leur parc informatique.

A ces deux éléments-clés, il faut ajouter des éléments propres à chaque entreprise, relatifs à son activité, à sa politique,…

Comme nous allons le voir dans les quelques schémas extraits de l'étude du CLUSIF, la question du budget est essentielle pour comprendre la facilité de certains hackers à pénétrer les systèmes et les pertes consécutives subies par les entreprises. Car si une protection informatique effective sera

---

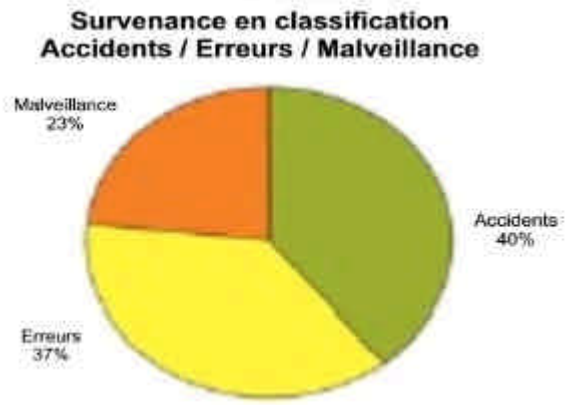
[17] Clusif, *Etudes et statistiques sur la sinistralité informatique en France. Année 2000*, mai 2001 (disponible à l'adresse http://www.clusif.asso.fr/fr/production/sinistralite/)

[18] L'important n'étant pas les chiffres mais les conclusions que l'on peut tirer de cette étude, le fait qu'elle ait lieu en France ne présente pas de problème pour notre sujet.

[19] L'enquête a été réalisée auprès de 450 entreprises et organismes publics : 400 enquêtes auprès de PME, sur la base d'un questionnaire auto-administré envoyé par fax après un contact téléphonique préalable permettant l'identification d'un interlocuteur compétent, et 50 enquêtes en face à face auprès de grandes structures, entreprises et administrations, sur la base d'un questionnaire similaire afin d'assurer la comparabilité des résultats, enrichi d'un recueil plus qualitatif sur la perception du risque par les RSSI (Responsables informatiques de l'entreprise).

pratiquement inefficace devant une erreur de manipulation ou un sabotage physique[20], elle permettra néanmoins d'éviter près d'un quart des risques encourus par l'entreprise, comme nous le montre le premier schéma.

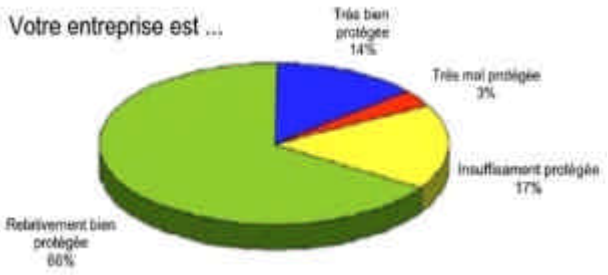
Le schéma suivant nous donne le pourcentage d'entreprises ayant subi un risque déterminé.

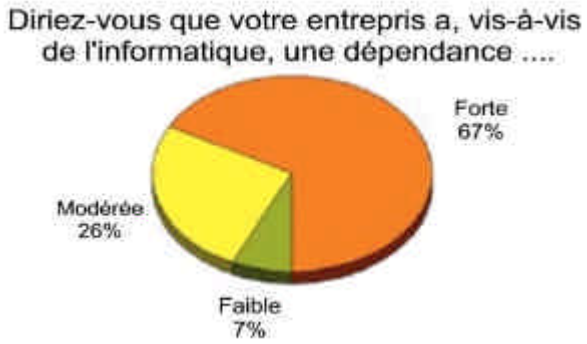


L'analyse de ce schéma pourrait tendre à minimiser le problème posé par le piratage informatique. Mais lorsque l'on sait que les 23% d'entreprises déclarant avoir été victimes de malveillances représentent près de 400000 entreprises en France, la lutte contre la hacking devrait être une des priorités majeures du budget « sécurité » au sein de l'entreprise.

Les schémas suivants vont permettre de pointer les deux éléments cités plus hauts comme explications de la perméabilité des systèmes de sécurité : l'impression de domination et la faiblesse du budget alloué.

Les deux premiers schémas nous montrent que 80% des entreprises se sentent relativement bien ou très bien protégées,…





… tout en ayant conscience qu'elles sont fortement ou modérément dépendantes vis-à-vis de l'informatique (et donc susceptibles d'être victimes de dégâts informatiques).

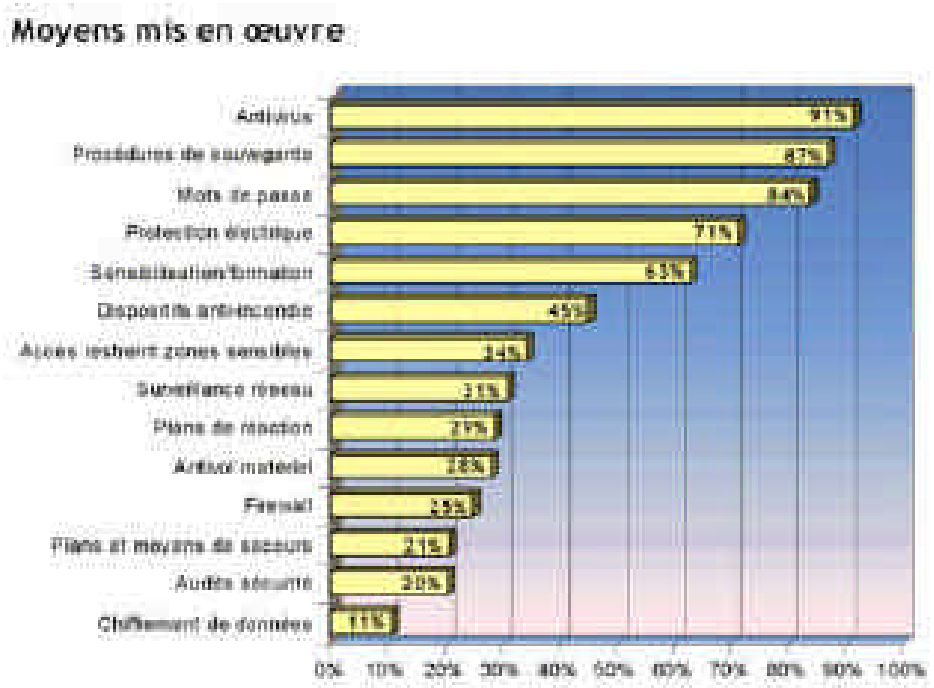
[20] Nous visons ici l'individu qui détruit physiquement les données (disques durs, CD-Roms, disquettes,…).

Cette dépendance vis-à-vis de l'informatique, et la vulnérabilité qui l'accompagne, découlent de règles simples[21] :

- Toute entreprise gère sur ses ordinateurs des fichiers automatisés contenant des informations sensibles ou stratégiques :
- Tout système informatique et ses réseaux comportent une ou plusieurs failles qui permettent de contourner le système de sécurité ;
- Toute personne ayant accès au système d'information a vocation à découvrir les faiblesses des dispositifs en place.

Si les entreprises s'estiment relativement bien ou très bien protégées, leurs modes d'actions ne sont pour autant pas des plus fiables. Ainsi, si les antivirus, les mots de passe et les procédures de sauvegarde sont utilisés dans 90% des entreprises, moins de 30% d'entre elles se protègent efficacement contre les pirates informatiques, négligeant ainsi de restreindre l'accès aux zones sensibles, de procéder à la surveillance du réseau, l'établissement d'un plan de réaction, de l'utilisation d'un firewall, le recours aux audits sécurité et au chiffrement de données).

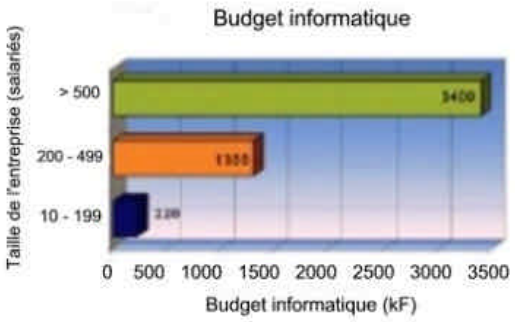
De plus, si trois quarts des entreprises disposent de protections électriques, moins d'une entreprise sur deux est équipée de dispositifs anti-incendie !

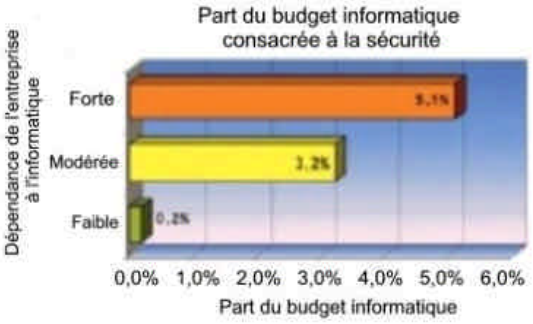


Enfin, si ce schéma nous renseigne sur la quantité des moyens de protections mis en place, il ne nous donne aucune indication sur la qualité de ceux-ci (fréquence des mise à jour des antivirus, complexité des mots de passe, …).

[21] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 38.

Concernant le budget, nous constatons que même dans les entreprises qui déclarent elles-mêmes que leur dépendance vis-à-vis de l'informatique est forte, cette prise de conscience ne s'accompagne pas des mesures suffisantes, le budget sécurité ne dépassant pas les 6% du budget informatique !





Ce rapide survol des risques encourus par les entreprises nous montre bien que, si ceux-ci sont relativement bien connus, en ce compris les dégâts qu'ils peuvent causer, la réponse des entreprises sur le plan budgétaire permettant de réduire l'impact des malveillances se fait toujours attendre.

Il est évident que la protection vis-à-vis des risques informatiques ne doit pas se limiter au budget (nous verrons ainsi, dans la partie consacrée à la prévention, que la sensibilisation du personnel est indispensable, eu égard aux dégâts causés par les malveillances et les erreurs humaines), mais il n'en reste qu'une si faible proportion traduit une relative sous-estimation des risques, alors que, encore une fois, le danger que ceux-ci représentent est connu !

Il est certain qu'un faible niveau de protection entraîne une perméabilité plus grande du système, si bien que la sous-estimation des risques est dès lors un facteur accroissant la possible action des hackers.

De même qu'une maison ne disposant pas de système de sécurité sera une cible intéressante pour un voleur, les entreprises, les systèmes mal protégés seront « privilégiés » par les pirates, et d'autant plus si l'entreprise, l'institution est connue. Ainsi, l'intrusion sur le site de la NASA, du Pentagone, … sont autant de sources de fierté, de reconnaissance pour le pirate, et ce, sans même tenir compte de la valeur des informations qu'il peut y trouver.

Bien sûr, d'importants moyens de sécurité peuvent être perçus comme un défi à relever pour les hackers les plus aguerris (les « Elites »[22]), mais ils permettront surtout d'éviter que les autres hackers, les « petits », ne puissent pénétrer leurs systèmes[23].

---

[22] Les Elites sont les hackers les plus doués, comme nous le verrons dans la partie consacrée aux différentes catégories de hackers.

[23] Nous reviendrons sur ces considérations plus tard dans la partie consacrée à la prévention.

Titre II – Le réseau Internet

L'analyse du réseau Internet[24] nous paraît essentiel en raison de son rôle déterminant dans le développement des hackers et de leurs méthodes de piratage, celui-ci permettant aux pirates tantôt de commettre les infractions, tantôt de se réunir, voire de coordonner des actions distantes de plusieurs milliers de kilomètres.

A ce titre, précision d'emblée que les considérations concernant les contrats électroniques, la problématique du commerce électronique, des sites pornographiques, celle des hébergeurs de sites Internet,.. ne seront pas ou peu abordées ici. De même, nous n'aborderons pas de détails trop techniques, comme le fonctionnement du protocole TCP/IP, du langage HTML, Java,… ceux-ci n'ayant pas d'intérêt pour une étude criminologique de la délinquance informatique.

Considérer l'Internet comme une révolution technologique est paradoxal lorsque l'on sait qu'il s'agit en réalité d'une invention vieille de 30 ans ! Il faut dire que l'Internet, inventé dans les années 60, ne fait partie de notre vie quotidienne que depuis un peu moins d'une dizaine d'années. Pourquoi une telle innovation, considérée aujourd'hui comme majeure, ne s'est-elle pas imposée plus tôt ? C'est ce que nous tenterons de comprendre à travers l'historique du réseau Internet. Nous y soulignerons les éléments déterminants qui ont permis à l'Internet de s'ouvrir au « grand public », alors qu'il était tout d'abord réservé à une élite.

Ensuite, nous présenterons quelques statistiques permettant d'avoir une idée de l'importance prise par le réseau Internet dans le monde, en particulier au regard du nombre d'internautes connectés. Ce sera pour nous l'occasion d'aborder les raisons de son succès grandissant, après avoir explicité les principaux services et applications que propose le réseau Internet.

Enfin, nous terminerons par quelques considérations juridiques relatives à l'Internet.

---

[24] « Internet » (sans article) est le nom du protocole de communication TCP-IP, alors que « l'Internet » (avec article) représente l'ensemble des réseaux interconnectés indépendamment de leur protocole.

Section 1 - Historique

Pour réaliser cet historique, nous nous sommes basés sur l'analyse de plusieurs sites Internet consacrés à ce sujet[25]. Cette décision est principalement motivée par l'actualisation régulière de ces sites en ligne, ce qui nous semble indispensable à l'analyse du phénomène en constante progression, voire transformation, qu'est l'Internet[26].

L'Internet est aujourd'hui le plus gros réseau informatique mondial[27]. Mais c'est surtout un réseau informatique ouvert[28] : ses utilisateurs ne se limitent pas à des personnes remplissant des conditions d'appartenance à des groupes déterminés[29].

L'Internet a connu des formes diverses, correspondant aux différents états de son développement, constituant ainsi l'illustration des avancées technologiques des trente dernières années, depuis l'invention du microprocesseur jusqu'aux réseaux mondiaux, planétaires.

A. LA NAISSANCE : DU SPOUTNIK À L'UNIVERSITÉ

On peut dater de 1968 la naissance du premier réseau informatique, connectant plusieurs ordinateurs. Cette année-là, la Grande-Bretagne, et plus particulièrement les National Physical Laboratories mettent au point le premier réseau à « commutation de paquets »[30], technologie fondée sur le découpage en paquets de l'information numérisée, afin de la faire mieux circuler.

---

[25] O., KAMGA, « L'autorégulation de l'Internet et ses répercussions sur le rapport entre les institutions publiques et les citoyens », http://www.er.uqam.ca/nobel/d364101/regulation.shtml, 31 août 2000 ; X, « Historique d'Internet », WebEncyclo (http://www.webencyclo.com/dossiers/sponsors/wanadoo/contenu/histoire1.asp), 2002 ; X, « Petite histoire d'Internet », Le Monde Interactif (http://interactif.lemonde.fr/article/0,5611,2860-5259-45838-0,FF.html), s.d. ; X, « Les bâtisseurs d'Internet », Le Monde Interactif (http://interactif.lemonde.fr/article/0,5611,2860-5259-154682-0,FF.html), s.d. ; R., ZAKON, « Hobbes' Internet Timeline v5.6 », http://www.zakon.org/robert/Internet/timeline/, 1er avril 2002 ; J.-C., PATAT,, « Guides du Net », http://patat.isdnet.net/net/indexbis.html, s.d.

[26] De même, les auteurs des articles ou dossiers, de par leurs qualifications, nous semblent donner les garanties nécessaires à une bonne compréhension de l'Internet.

[27] Un réseau informatique est un ensemble de matériels informatiques interconnectés, formé de nœuds (les serveurs ou ordinateurs clients), et de liens (les lignes téléphoniques, les câbles, la fibre optique ou encore les connexions par satellite).

[28] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 67.

[29] A contrario, le réseau informatique fermé est limité à certains groupes d'utilisateurs, comme les employés d'une entreprise par exemple.

[30] Le principe est le suivant : au départ, le message est divisé en blocs (les paquets), transmis à travers les branches du réseau ; à l'arrivée, les destinataires rassemblent les blocs et reconstituent le message.

C'est aux Etats-Unis que l'idée d'un réseau mondial utilisant la technique de la commutation de paquets va être intensément développée. Dès 1957, le Ministère de la Défense américain crée l'Agence ARPA (Advanced Research Project Agency) dont l'objectif est de renforcer les développements scientifiques susceptibles d'être utilisés à des fins militaires.

Mais d'autres raisons motivent également ces recherches. Une certaine polémique attribue la paternité d'Internet à l'armée américaine. Le lancement du Spoutnik venait d'avoir lieu, et les Etats-Unis voulaient réagir, afin de ne plus jamais être dépassés par l'URSS dans le domaine des télécommunications.

En effet, en cette période de Guerre Froide, les systèmes de télécommunication sont fondés sur la technologie des réseaux téléphoniques centralisés. Dès lors, une attaque nucléaire sur les points centraux névralgiques rendrait l'utilisation du réseau impossible. Les chercheurs américains ont par conséquent pour mission la mise en place d'un réseau de communication militaire capable de résister à ce type d'attaques.

C'est en 1969 que des chercheurs parviennent à relier entre eux quatre des ordinateurs de University of California in Los Angeles (UCLA). L'Arpanet était né. Ce réseau est fondé sur une structure de réseau maillé, chaque nœud du réseau étant relié aux autres, sans qu'aucun centre ne concentre l'information. La communication entre les différents nœuds est assurée par la commutation de paquets, ce qui garantit le bon fonctionnement du réseau, même si l'un des nœuds vient à défaillir[31].

Comme il n'existe pas de point central par lequel les messages sont obligés de transiter, le réseau continue de fonctionner, même en cas de destruction partielle. Cette idée de décentralisation est à la base du premier réseau mondial, comme elle le sera encore pour l'Internet.

En 1972, a lieu à Washington la première conférence internationale sur les communications informatiques, au cours de laquelle une démonstration d'Arpanet est organisée devant de nombreux spécialistes venus du monde entier. C'est à partir de ce moment que vont commencer des discussions entre plusieurs pays qui travaillent sur des projets de réseaux à commutation de paquets.

Dès 1973, des pays comme la France ou la Grande-Bretagne travaillent à l'élaboration de leur propre réseau informatique, tous ressentant alors le besoin de créer un protocole de communication commun à tous ces réseaux.

En 1974 est créé l'Internetwork Working Group, chargé d'élaborer ce protocole commun. Dans ce groupe se trouvent deux chercheurs de l'UCLA, Vinton Cerf et Robert Kahn, qui vont élaborer un protocole spécifique aux communications inter-réseaux (en anglais INTER-NETwork) compréhensible par tous les ordinateurs. Ce protocole, langage commun à tous les réseaux, toujours utilisé aujourd'hui, se nommera TCP-IP (Transmission Control Protocol, Internet Protocol). L'Internet était né.

Il est à ce titre intéressant de voir que, dès sa création, le réseau Internet ne peut être limité à sa dimension technologique. Son inscription idéologique dans l'Histoire montre à quel point sa dimension politique est importante. Dépassant son statut de média mondial, l'Internet incarne la vision d'un système qui, outre la technologie, concerne la politique, l'économie et l'organisation-même de la société. L'idée d'un réseau décentralisé, sans hiérarchie, reprend l'idéologie libérale américaine, avec l'idée que même dans l'hypothèse d'un réseau anarchique, les éléments qui le composent finiront nécessairement par le réguler. A l'époque, cette vision est directement opposable à l'idéologie soviétique de centralisme démocratique, dans laquelle le pouvoir est concentré et où toute diffusion d'information est soumise à ce pouvoir.

L'influence des milieux universitaires de la fin des années 60 et des années 70 marquera les premiers pas libertaires de l'utilisation du Web en tant que média.

[31] L'idée de réseau maillé provient de l'Américain Paul Baran à qui l'US Air Force avait demandé d'améliorer les systèmes de communications militaires.

B. L'OUVERTURE AU PUBLIC : LE WORLD WIDE WEB

Durant les années 80, l'usage de l'Internet se limite principalement à l'échange de courriers électroniques et de fichiers entre les universités du monde entier.

Ce n'est qu'en 1989, grâce à la création du World Wide Web (WWW) par Tim Berners-Lee, un physicien britannique travaillant pour le CERN (Organisation Européenne pour la Recherche Nucléaire), que l'Internet va commencer à conquérir le grand public. L'idée du Web est née du besoin de trouver un nouveau système pour gérer les multiples documents édités par le CERN, ces documents comportant beaucoup de graphiques, équations et autres dessins techniques. Le Web sera donc, dès sa création, multimedia, puisqu'il permet très tôt d'associer des contenus sous forme de texte, d'image et de son.

Ces documents doivent également être accessibles en tout temps et en tout lieu, pour répondre au besoin des chercheurs de partager leurs informations et documents où qu'ils soient[32].

Tim Berners-Lee invente et rassemble trois éléments fondamentaux qui forment le World Wide Web.

Tout d'abord, le protocole d'hypertexte, Hypertext Transfer Protocol, représenté aujourd'hui par le symbole HTTP. Ce standard permet aux ordinateurs de lier les documents entre eux.

Il crée également l'Uniforme Ressource Locator (URL), qui va permettre de trouver un document en tapant simplement une adresse (www.yahoo.com).

Enfin, il introduit le langage HTML (Hypertext Markup Language), qui permet de créer des documents multimédia sur le Web et de les relier grâce à l'hypertexte.

Berners-Lee va ainsi, grâce à l'invention du World Wide Web, créer la première librairie mondiale, permettant à l'Internet de conquérir le grand public[33].

C. LA DÉMOCRATISATION INFORMATIQUE

En 1990 naissent les premiers serveurs (c'est-à-dire les sites hébergeant les informations et les liens) et les premiers butineurs, ou browsers (il s'agit de logiciels de navigation permettant de lier et de parcourir les informations sur le Web).

En 1993, le butineur Mosaic est élaboré au NCSA (Centre National pour les Applications des Super-ordinateurs) aux États-Unis. Très vite, la NCSA va produire des versions de ce logiciel pour

---

[32] A cette époque, le CERN travaille à la construction d'un gigantesque accélérateur de particules, le LEP (Large Electron-Positron collider), et ce projet nécessite une étroite collaboration internationale entre tous les scientifiques.

[33] Nous tenons à préciser que lorsque nous parlerons d'Internet, ce sera au sens large, en ce compris le Web, les différents protocoles, standards utilisés, les différents modes de transferts de fichiers,….

les Macintosh et les PC, sous le nom de « NCSA Mosaic », ouvrant la porte du Web et de l'Internet au grand public grâce à la convivialité qu'offre le logiciel, celui-ci permettant en effet l'affichage d'images en couleurs.

En 1994, Jim Clark, l'un des dirigeants de Silicon Graphics, décide de racheter Mosaic et développe à partir de celui-ci une interface performante et évolutive, capable d'être utilisée par le grand public : Netscape. Lancé à la fin de l'année 1994 et distribué gratuitement sur le Web, (comme l'avait été Mosaic), Netscape va rapidement être adopté par de nombreux utilisateurs du Web au point de devenir une norme. Même si la majorité des utilisateurs recourent désormais à son concurrent Microsoft Internet Explorer (notamment en raison de son intégration dans le système d'exploitation de Microsoft Windows), le navigateur de Netscape a longtemps occupé la place de leader.

A la fin de l'année 1994, on recensait 10 millions d'utilisateurs du Web à travers le monde. Aujourd'hui ils seraient près de 500 millions.

C'est donc bien le Web qui a permis l'accès du grand public à l'Internet. Celui-ci s'était développé depuis 30 ans dans le cadre de communautés scientifiques dont les objectifs étaient très éloignés des préoccupations économiques ou commerciales. Avec le Web et les premiers logiciels de navigation, des personnes étrangères au monde scientifique ont commencé à se connecter au «réseau des réseaux », transformant profondément son contenu et son mode de fonctionnement. Chercheurs et étudiants vont le rendre plus ludique et plus attractif, créant leurs propres sites ainsi que les premiers moteurs de recherche et annuaire tels Altavista ou Yahoo!. Lancé officiellement en mars 1995, Yahoo! référence à l'origine les sites préférés des ses deux fondateurs, Jerri Yang et David Filo, tous deux étudiants de Stanford.

Ce sont également eux qui fondent la netiquette, charte éthique du comportement des internautes, toujours en vigueur aujourd'hui. La netiquette prône, dans un contexte de «libre expression », des valeurs telles que le respect mutuel, l'échange et le partage d'informations, le désintéressement... Même si l'un des principes fondamentaux de la netiquette « pas d'argent sur Internet » a volé en éclat ces dernières années avec la généralisation du e-Business, la netiquette demeure : les forums restent des places d'échanges mutuels, où les modérateurs font respecter des chartes établissant les sujets et les modes d'interventions propres à chaque forum[34].

Toutes ces innovations nées des premiers internautes (annuaires de recherche, navigateurs, etc.) rendent de plus en plus convivial l'accès au réseau. Elles favorisent l'accès des particuliers au Web et attirent de nouveaux entrepreneurs sur l'Internet, qui entame ainsi une sorte de seconde carrière où le

[34] V., SHEA,, « Netiquette », http://www.albion.com/netiquette/book/index.html, 1994.

business prend une place de plus en plus importante. Elément essentiel du réseau, le e-Businness fait désormais en grande partie vivre l'Internet, depuis que celui-ci n'est plus uniquement utilisé par la communauté scientifique.

Mais il est évident que parmi ces étudiants et chercheurs un peu fous, se trouvent bon nombre de pirates informatiques. Nous verrons dans la partie qui leur est consacrée, que contrairement à ce que l'on pourrait croire de prime abord, les pirates informatiques ne cherchent pas uniquement la destruction des données (au sens large). Ce serait même plutôt le contraire.

Il faut bien avoir à l'esprit que les pirates ont également fait évoluer l'Internet. Ceci nous amène à souligner que Durkheim avait déjà avancé l'idée selon laquelle le crime était normal.

Selon lui, le crime est normal car il se manifeste dans toutes les sociétés et il ajoute qu'il est même un facteur de santé publique. Il ajoutera le crime est inévitable et utile[35].

Ce constat peut également être appliqué au réseau Internet, où le crime informatique, comme en témoigne le présent travail, est une réalité. Sur le Net, le crime est également inévitable et utile.

• Le crime est inévitable :

Internet était d'abord développé dans un but scientifique, afin de faciliter l'échange de données. Rapidement, des individus se sont écartés de cette optique collective pour récupérer Internet et les opportunités qu'il proposait à leur avantage, pour leurs propres intérêts, faisant d'eux des marginaux et donc, parfois, des criminels.

· Le crime est utile :

Le crime informatique a une utilité *directe* dans l'évolution de la morale et du droit. Comme nous le verrons, la majorité des pirates informatiques revendiquent un Internet libre. Libre de droit, libre de censure, libre de consultation.

Ce mouvement contestataire est à la base de nombreux actes de piratage, amenant ainsi le réseau à repenser sa politique et à remettre en cause la légitimité de ses acteurs et de leurs actes.

On verra ainsi différentes chartes, comme la netiquette, fleurir sur le Net, expliquant ce que l'on peut et ne peut pas faire sur le Web. Dans le même esprit, de nombreux sites arborent le « blue ribbon » sur leurs homepages, exprimant ainsi leur solidarité envers ceux qui revendiquent un Internet libre de toute censure. Toutes ces initiatives sont l'œuvre du réseau et des ses acteurs eux-mêmes, procédant ainsi à une véritable autorégulation.

---

[35] R., GASSIN, *Précis de criminologie*, Paris, Dalloz, 1994, p. 128.

Ensuite, le crime informatique présente une utilité *indirecte*. Consécutivement aux actes de piratages, de nombreux sites se sont créés afin de permettre de se protéger de ce type de malveillances. C'est ainsi par exemple le cas du site www.zataz.com, qui réunit des interviews de hackers (repentis ou non), des dossiers sur les différentes formes de piratages et de virus, ainsi que des outils informatiques de protection.

De même, sans les pirates informatiques, il n'y aurait pas de programmes d'anti-virus, pas de firewalls, pas de cryptologie informatique, pas de mots de passe,… et la liste est encore longue. Bien entendu, nous serions tentés de dire que ces systèmes n'auraient aucune utilité si les pirates n'existaient pas. En réalité, il n'en est rien car les pirates ont simplement jouer le rôle de catalyseur pour le développement de logiciels qui devaient, à terme, être élaborés afin d'assurer des échanges seriens sur le réseau. Ainsi, il n'est pas besoin d'être un pirate que pour lire un e-mail confidentiel qui serait, par erreur arrivé dans votre boîte mail, tout comme les firewalls permettent également de limiter les consultations du réseau Internet à certains sites (ce qui est utile, par exemple, pour les entreprises désireuses de ne pas voir leur personnel passer leur temps de travail à surfer sur le web).

Si les pirates informatiques ont pris le train des nouvelles technologies en marche, ils ne se sont pas pour autant contentés d'être des spectateurs passifs. Ils ont contribué au développement d'Internet et à son évolution morale, technique et juridique.

L'Internet et le Web, à l'image de nombreuses innovations, ont été adoptés successivement par différents précurseurs avant d'aboutir au grand public. Dans le cas de l'Internet, ces précurseurs (« forerunners ») ont été les militaires et les scientifiques, les innovateurs (« early adopters ») ont principalement été des étudiants et des professionnels de l'informatique. Aujourd'hui, si l'Internet est arrivé au stade de la diffusion « grand public », cette étape est loin d'être achevée car les utilisateurs de ce média sont encore dans leur grande majorité des membres d'une certaine « élite » socioprofessionnelle et culturelle (ne serait-ce que par la nécessité d'avoir accès à un ordinateur et l'obligation de savoir l'utiliser).

Le développement de l'informatique domestique a également favorisé l'accès au Web. La baisse des prix des ordinateurs et des modems est encore un moteur à la multiplication des connexions à l'Internet. La libéralisation progressive du domaine des télécommunications, aux États-Unis puis en Europe, a permis à l'Internet de se développer en dehors des circuits restreints dans lesquels il avait été créé puis exploité. Ainsi, la technologie ADSL (Asynchronous Digital Subscriber Line : débit numérique asymétrique sur ligne d'abonné) permet de « surfer » plus rapidement, permettant de télécharger des fichiers de plus en plus volumineux, faisant de l'Internet le premier fournisseur d'informations, de quelque type que ce soit (textes, sons, images, vidéos,…). Enfin, la multiplication de nouveaux services en ligne gratuits (journaux, informations, logiciels...) a fini d'attirer le grand public.

D. INTERNET II : LE RETOUR

Plusieurs axes semblent se dessiner pour les futurs développements du réseau Internet. Depuis quelques années déjà, les universités américaines étudient « l'Internet II ». Ce nouveau réseau, reprenant les principes de fonctionnement du premier, apporte notamment de nouvelles architectures et des protocoles optimisés, qui devraient permettre aux utilisateurs d'accéder au réseau dans de meilleures conditions que celles dont ils bénéficient actuellement.

Il faut également souligner que l'Europe est en avance sur les Etats-Unis dans certains domaines comme le WAP[36] (Wireless Application Protocol). C'est la rapide normalisation des réseaux de télécommunications sans fil au niveau européen qui a permis cette domination au niveau international. Reste à savoir si le WAP rencontrera le succès escompté…

Les autres nouveautés s'intègrent dans ce qu'on appelle désormais la « convergence des médias ». Il semble en effet que le développement d'un réseau mondial, Internet ou autre, passe par la multiplication et la simplification des terminaux de consultation. On imagine facilement des applications pour le domicile (domotique) ou pour la voiture (guidage par satellite).

Le réseau Internet ne peut pas être appréhendé en tant que fin en soi. Il s'agit plutôt d'analyser son succès comme participant d'une Révolution industrielle entamée il y a une quarantaine d'années avec l'invention du transistor et de l'électronique, et menant progressivement les économies industrielles vers des économies de l'information.

[36] Il permet d'utiliser des applications à distance sur des terminaux sans fils comme les téléphones portables ou les PDA (Portable Digital Assistant), et donne accès à un « Internet simplifié », limité aux services généraux comme la météo, la consultations de résultats sportifs,…

E. CHRONOLOGIE DES ÉVÉNEMENTS

Pour finir, nous livrerons ici un rapide récapitulatif des dates les plus marquantes de la création et du développement du réseau Internet.

- Début des années 60 : Dans le cadre du programme ARPA, les militaires américains décident de créer un réseau de communications capable de résister à une attaque nucléaire. Le concept était basé sur un système décentralisé, continuant de tourner si un élément était touché.

- 1969 : Le réseau Arpanet relie quatre universités. On considère souvent que c'est la date de naissance de l'Internet.

- 1972 : Création du premier courrier électronique, afin de répondre aux besoins des développeurs du réseau Arpanet. D'autres applications vont rapidement suivre comme les forums et le FTP (File Transfer Protocole).

- 1973 : Début de l'expansion internationale avec la connexion du réseau à la Suède et à la Norvège.

- 1974 : Création du protocole TCP/IP qui permet à des ordinateurs de types différents de communiquer au sein d'un réseau, en fragmentant les données par petits paquets, plus faciles à transporter.

- 1989 : Premier échange commercial sur Internet.

- 1990 : Création du « système hypertexte » (HTML) au CERN, à Genève.

- 1993 : L'élaboration du premier browser graphique, Mosaic, ancêtre de Netscape, et sa diffusion gratuite ouvrent l'Internet au grand public.

- 1995 : Création du premier portail[37] (ou moteur de recherches), Yahoo! ; de la première librairie en ligne, Amazon.com ; Geocities est le premier hébergeur gratuit de pages web ; Internet Explorer est fourni gratuitement par Microsoft avec son système d'exploitation Windows.

- 2001 : On estime à plus de 500 millions le nombre d'internautes au niveau mondial.

[37] Ce terme est utilisé afin de représenter l'idée d'une porte d'entrée dans le réseau Internet.

Section 2 - Principales applications

Le réseau Internet n'est pas uniquement limité à la conception et la consultation de sites Internet. Il favorise également les échanges entre internautes, principalement au moyen des applications suivantes[38] :

• Le courrier électronique (E-mail)

L'E-mail (Electronic Mail) ou courrier électronique est un service qui utilise le réseau Internet pour véhiculer des messages écrits entre un expéditeur et un destinataire.

• Le World Wide Web (WWW)

Le WWW peut être défini comme un service d'Internet qui assure la mise à disposition d'informations de tout genre sous un format convivial pour toutes les personnes connectées et/ou par toutes les personnes connectées.

Le Web est né en 1989 au Centre Européen de Recherche Nucléaire (CERN) de Genève lors du développement du protocole HTTP. Mais son véritable succès ne se précise effectivement qu'à partir de 1993, date à partir de laquelle le trafic des données et le nombre de machines connectées croissent de manière exponentielle.

• Les News, forums ou groupes de discussion

Il s'agit d'un système de discussion mondialement distribué, reprenant un ensemble de groupes de discussions nommés et classés hiérarchiquement (les *rubriques*) dans lesquels les utilisateurs du système peuvent poster des messages (les *articles*) qui sont diffusés par les serveurs de News.

Dès que le message est diffusé, n'importe quel utilisateur connecté à Internet peut alors lire le message en se connectant sur un serveur de News reprenant la rubrique visée et en lisant les messages postés dans cette rubrique.

• L'Internet Relay Chat (IRC)

L'IRC (Internet Relay Chat) est un système de conversation multi-utilisateurs où les utilisateurs se rassemblent dans des canaux pour parler en groupe ou en privé. Cette communication se fait en temps réel.

---

[38] S., GHERNAOUTI-HELIE, *Sécurité Internet, Stratégies et technologies*, Paris, Dunod, 2000, p.17.

Section 3 - Internet en chiffres

Nous allons ici livrer quelques tableaux statistiques[39] reprenant les activités liées à l'Internet dans le monde. Ces chiffres ont pour but de montrer que l'Internet est devenu une partie essentielle des champs économique, culturel, juridique, médical,… et partant, les infractions qui se réalisent au travers d'Internet ou grâce à Internet pourront également se développer et s'étendre dans tous ces domaines.

Le premier tableau, que nous ne présentons que partiellement, représente le nombre d'Internautes dans le monde. Celui-ci a pour but, non pas de faire une comparaison entre chaque pays du nombre d'internautes (pour laquelle il faudrait tenir compte des différences de populations), mais de montrer que l'utilisation de l'Internet est loin d'être un phénomène marginal.

Comme nous pouvions nous y attendre, ce sont les Etats-Unis qui prennent la première place (plus de 60% des infrastructures de l'Internet se trouvent aux Etats-Unis[40]), la Belgique pointant à la 19e place, avec 2,7 millions de Belges connectés.

Internautes dans le monde par pays (en millions)(mai 2002)			
Pays	**Population totale**	**Nombre d'Internautes**	**Internautes actifs** (càd se connectant au moins une fois par jour)
Etats-Unis	278,0	166	106,7
Chine	1,3	56,6	-
Japon	126,8	51,9	20
Allemagne	83	32,2	18,0
Grande-Bretagne	59,6	29,0	16,5
Russie	145	18	8
Canada	31,6	16,8	10,4
France	60	14,6	8,4
Italie	57,7	11,0	8,3
Australie	19,4	10,6	6,3
Pays-Bas	16	9,5	5,4
Espagne	40,0	7	4
Brésil	174,5	6,1	6,0
Suède	8,9	5,9	3,8
Turquie	66,5	3,7	-
Argentine	37,4	3,6	--
Suisse	7,3	3,4	1,8
Danemark	5,4	3,3	2,0
Belgique	10,3	2,7	1,6
Norvège	4,5	2,5	1,5

Sans surprise également, le continent américain compte le plus grand nombre d'internautes dans le monde, suivi par l'Europe et l'Asie. Bien que le continent américain ne soit pas le plus peuplé, ceci

[39]Ces tableaux sont extraits du site du Journal du net, www.journaldunet.com (les notes concernant les adresses Internet ne contiendront généralement pas de date précise, ceux-ci étant régulièrement mis à jour).

s'explique par le fait que, comme nous venons de le dire, plus de la moitié des infrastructures de l'Internet se trouvent aux Etats-Unis.

Internautes dans le monde par continent (mai 2002)	
Zones	**Nombre (en millions)**
Afrique	4,15
Asie/Pacifique*	143,99
Europe	154,63
Moyen Orient	4,65
Canada & USA	180,68
Amérique latine	15,33
Total Monde	513,41

Les schémas suivant sont présentés ici à titre purement informatif, toujours dans l'esprit d'avoir une vision globale du phénomène Internet.

Nombre de sites dans le monde		
Année	**Nombre de sites**	**Progression**
2001	8.745.000	+18%
2000	7.399.000	+52%
1999	4.882.000	+71%
1998	2.851.000	+82%
1997	1.570.000	-

Ce tableau montre bien la progression quasi-exponentielle du réseau des réseaux, qui en cinq ans, a vu le nombre de sites Internet être multiplié par plus de cinq.

Le Web comprend 8,7 millions de sites Internet dans le monde, dont 3,1 millions de sites ouverts au public.

Sur les 3,1 millions de sites publics, 47% sont américains, 5% allemands et moins de 2% sont français.

Répartition des sites publics dans le monde par catégorie	
Type de site	**%**
Information	15,5%
Services professionnels, scientifiques, techniques	14,2%
Autres services	12,8%
Commerce	11,8%

[40] P., SABATIER, « Crimes sur le Net », www.liberation.fr, 12 décembre 1997.

Enfin, sur l'ensemble des sites répertoriés, 73% d'entre eux sont en langue anglaise.

Industrie	8,5%
Education	6,6%
Culture et loisirs	4,7%
Alimentation et autres biens de consommation courante	2,8%
Immobilier	2,3%
Finance et assurance	2,1%
Autres	9,6%
Non identifiés	9,1%

Comme le montre les chiffres qui viennent d'être présentés, le réseau Internet connaît un succès grandissant.

Les raisons de ce succès sont, consécutivement à ce que nous avons vu dans l'historique qui lui est consacré, de deux ordres : technologique et juridique[41].

- **technologique :** l'apparition de processeurs plus puissants, de disques durs plus grands et surtout de moyens de connexion toujours plus performants (modem ADSL, ISDN, connexion par câble,…), ayant permis de créer diverses applications propres au réseau Internet[42] (e-mail, IRC,…), sont ainsi autant de facteurs expliquant le développement du réseau et sa plus grande accessibilité.

- **juridique** : la libéralisation des télécommunications, déjà effective dans certains pays et prévue en Belgique, a donné naissance à une série d'opérateurs privés, proposant leurs conditions et modes d'accès propres.

La conjonction de ces deux types de facteurs va donner naissance à un troisième, que l'on pourrait qualifier de technico-juridique : la baisse des coûts des équipements et des communications.

La libéralisation a ouvert la voie à la concurrence et chaque opérateur voulant prétendre à des parts de marchés, il est devenu indispensable d'être compétitif, par tous les moyens.

A titre d'exemple, on peut citer Belgacom (ici dans son rôle de fournisseur d'accès) qui, voyant le succès remporté par Freebel (en 1999) et sa formule d'accès gratuit à Internet[43], a abandonné toute sa politique d'abonnement pour lui aussi proposer l'Internet « gratuit ».

---

[41] A., STROWEL, J.-P., TRIAILLE, *Le droit d'auteur, du logiciel au multimédia*, Bruxelles, Story scientia, Cahiers du Centre de Recherches Informatique et Droit, n°11, 1997, pp. 339 à 340

[42] Cf. supra.

[43] Freebel, www.freebel.be.

Section 4 - Cadre juridique

Dans un souci de concision, nous limiterons les explications relatives au cadre juridique du réseau Internet à la compréhension de notre exposé.

D'autres considérations, comme celles relatives au commerce électronique par exemple, s'écartant de notre sujet, ne seront pas abordées.

A contrario, le réseau Internet étant le théâtre de nombreuses infractions non spécifiques, comme la pornographie ou le hacking[44], nous aborderons celles-ci dans la partie consacrée à la loi du 28 novembre 2000 relative à la criminalité informatique, de même que les considérations relevant de la procédure pénale, comme les perquisitions sur le réseau.

Nous nous intéresserons donc exclusivement au respect des communications et, d'une manière générale, aux principes de droit pénal applicables au réseau Internet.

A. LE SECRET DES COMMUNICATIONS

Fondamentalement, le cadre juridique du réseau Internet est délimité par la loi du 21 mars 1991 portant réforme de certaines entreprises publiques et économiques dont le titre III a trait aux télécommunications[45].

Aux termes de l'article 68 de ladite loi, est considéré comme relevant des télécommunications *« toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radioélectricité, signalisation électrique ou un autre système électromagnétique »* [46].

Si le cadre juridique (général) du réseau Internet est ainsi posé, qu'en est-il de la législation applicable à ses applications propres, et en particulier aux e-mails ?

L'Internet est principalement un réseau de télécommunications. Dès lors, les communications étant privées, secrètes, ce qui se passe sur le réseau Internet l'est aussi, et donc, toute infraction à ce principe doit être réprimée par les articles 259bis et 314bis du Code pénal [47], introduits par la loi du

---

[44] Nous verrons plus tard que, contrairement à ce que l'on pourrait penser, le réseau Internet n'est pas indispensable à la commission de ce type d'infractions. Ainsi, à titre d'exemple, le cassage de code de sécurité peut se faire directement sur l'ordinateur visé, sans passer par le réseau Internet.

[45] Nous y reviendrons plus tard dans l'analyse consacrée à la loi du 28 novembre 2000 relative à la criminalité informatique.

[46] L. du 21 mars 1991 portant réforme de certaines entreprises publiques et économiques, *M.B.*, 27 mars 1991, p. 6155.

[47] P., VAN EECKE, *Criminaliteit in cyberspace*, Gand, Mys en Breesch, 1997, p. 42.

30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunication privées[48].

Si les e-mails que s'échangent deux internautes entrent évidemment dans cette acception, qu'en est-il des sites Web, où l'information est accessible, offerte au public ? Selon la doctrine, *« la sélection de la réception par un utilisateur d'Internet d'une information quelconque revêt un caractère privé, indépendamment du fait que cette même information soit accessible au public. La protection du secret des communications ou des télécommunications doit par conséquent s'appliquer à ce type d'échanges »*[49].

L'article 259bis concerne les officiers et fonctionnaires publics, dépositaire ou agent de la force publique, qui procéderait à des écoutes illégales.

L'article 314bis du Code Pénal, quant à lui, interdit aux opérateurs de télécommunications et aux fournisseurs d'accès de prendre connaissance ou d'enregistrer les communications qui s'opèrent par leur entremise et auxquelles ils ne peuvent directement prendre part.

Il y a cependant une brèche dans ce bel ensemble de garanties : le contenu des communications n'est protégé que durant le temps de leur transmission. Ainsi, s'il nous prend l'envie de pirater des dizaines d'e-mails et de les enregistrer sur notre disque dur pour les consulter plus tard, nous ne tombons pas sous le coup des dispositions pénales précitées[50].

A l'exemple de ce qui vient d'être exposé concernant le secret des communications et les e-mails, qu'en est-il de l'interprétation de la loi et de son applicabilité face à l'évolution constante du réseau ?

---

[48] L. du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunication privées, *M.B.*,10 mai 1995, p. 01542.

[49] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 75

[50] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 75

B. LES PRINCIPES DE DROIT PÉNAL APPLICABLES

Nullum crimen, nulla poena, sine lege. Ce principe de droit pénal met en évidence l'un des problèmes les plus récurrents posés par Internet : l'interprétation de la loi[51].

Par plusieurs arrêts, la Cour de cassation a montré la voie vers une interprétation évolutive de la loi. A titre d'exemple, on citera l'arrêt de la Cour de cassation du 4 mai 1988[52], qui énonce que le juge peut étendre l'application de la loi pénale à d'autres faits que le législateur était dans l'impossibilité de prévoir au moment de la promulgation de la loi, mais à deux conditions :

- la volonté du législateur d'ériger ces faits en infraction doit être certaine
- ces faits doivent entrer dans la définition légale de l'infraction[53]

Pour ce qui est des infractions commises via Internet par plusieurs personnes, elles peuvent se voir appliquer les articles 66 et 67 du Code pénal[54].

Enfin, Internet n'ayant pas réellement de frontière, le problème de la loi applicable à l'infraction ne sera pas nécessairement évident.

Au regard de la doctrine et de la jurisprudence (notamment de l'arrêt « Bologne »[55]), il apparaît que les juridictions belges seront compétentes pour connaître d'une infraction dès qu'un élément constitutif de cette infraction a été réalisé en Belgique[56].

---

[51] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 170.
[52] Cass., 4 mai 1988, *Rev. dr. pén.*, 1988, p. 958.
[53] Cass.25 janvier 1986, *Pas.*, 1986, I, p.534 + note ; Cass. 4 mai 1988, *R.D.P.C.*, 1988, p. 958 ; Cass. 11 septembre 1990, *Pas.*, 1991, I, p. 36 ; Cass. 15 mars 1994, *Pas.*, 1994, I, p. 261.
[54] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 172.
[55] Cass., 17 mai 1957, *R.C.J.B.*, 1957, p. 92.
[56] Cass. 16 mai 1989, *Pas.*, 1989, I, p. 973 ; H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 270.

Section 5 – Conclusion

Le réseau Internet, de par les spécificités qui viennent d'être présentées, joue un rôle déterminant dans le développement du piratage informatique.

En raison du nombre élevé de sites consacrés au hacking, des facilités offertes par les nouveaux moyens de communications proposés par l'Internet ainsi que leur grande rapidité, les apprentis hackers vont pouvoir se multiplier sur la « Toile », le hacking présentant désormais un aspect multinational.

Auparavant, comme nous le verrons dans l'historique consacré aux hackers, les apprentis pirates devaient apprendre par leurs propres moyens, bidouiller leur machines chacun de leurs côtés et se réunir « physiquement » pour confronter leurs dernières découvertes.

Le réseau Internet a balayé ces contraintes, si bien qu'il est tout à fait possible de contacter quelqu'un distant de plusieurs milliers de kilomètres, et ce en quelques secondes. Sur ce plan, l'Internet ne souffre aucune concurrence : aucun moyen de communication actuel ne permet de connecter, de contacter des personnes distantes l'une de l'autre avec autant de rapidité et pour un coût aussi faible. Il ne nécessite même pas de disposer d'un ordinateur personnel, les cybercafés fleurissant partout dans les villes.

Enfin, si le réseau Internet permet de se connecter à des personnes géographiquement éloignées, il permet avec tout autant de rapidité aux hackers de pirater un ordinateur se situant à l'autre bout de la planète, expliquant ainsi la relative impunité, consécutive de l'anonymat[57] – tout aussi relatif – dont ceux-ci peuvent jouir.

[57] Il est entendu que l'anonymat du hacker dépendra de l'ingéniosité développée par le hacker pour effacer ses traces et de l'habilité des autorités à retrouver celles-ci.

Titre III – Les caractéristiques de la criminalité informatique

Depuis une vingtaine d'années, la généralisation de l'informatisation a accru la vulnérabilité des entreprises, des états, et avant tout des particuliers, face aux risques.

Cette vulnérabilité est liée aux caractéristiques de l'informatisation même : complexité des systèmes, coûts des équipements et des logiciels, …

La criminalité informatique n'est pas limitée aux quelques exploits individuels relatés par les médias, mais est beaucoup plus complexe, étant donné que l'informatique est « en tout » et surtout « partout ».

Cette complexité s'explique par différentes raisons.

Tout d'abord, la définition de la criminalité n'est pas unique, plusieurs auteurs ayant donné leur propre vision de ce concept.

De même, comme nous le verrons, la place de la criminalité informatique par rapport aux autres formes de criminalité n'est pas sans poser de questions.

Ensuite, la mesure de cette criminalité, ainsi que son coût, posent également problème, les pertes engendrées étant, entre autres, souvent dissimulées par les victimes elles-mêmes (par exemple afin de garantir le prestige de la société victime de l'acte délinquant).

Nous commencerons cette partie par tenter de définir ce que recouvre la notion de «criminalité informatique ». Pour cela, nous confronterons les diverses définitions élaborées, avant d'aborder les similitudes et les différences existant entre la criminalité informatique et la criminalité en col blanc.

Ensuite, nous expliquerons pourquoi l'étendue de la criminalité informatique est difficilement déterminable, nous attardant ici sur les différentes sources d'informations, tant nationales que nationales, sur ce phénomène. Ce sera l'occasion d'analyser les exemples à suivre et à ne pas suivre, que sont respectivement la Business Software Alliance et le Cybercriminstitut.

Nous apporterons également des éléments d'explication de l'importance du chiffre noir dans l'évaluation de la criminalité informatique.

Enfin, nous terminerons cette partie en pointant quelques éléments permettant de comprendre l'importance des coûts engendrés par la criminalité informatique, les considérations juridiques relatives à celle-ci étant abordées plus tard dans l'analyse de la loi du 28 novembre 2000 relative à la criminalité informatique.

Section 1 – La notion de « criminalité informatique »

A. DÉFINITIONS

Bien que les notions de «criminalité informatique » et de «cybercrime » (ou «cybercriminalité ») sont étroitement liées, il existe néanmoins une distinction entre les deux conceptions.

Ainsi, la criminalité informatique représente l'infraction générique, dont le cybercrime est une variante. Nous basons cette distinction sur la définition générale de la criminalité informatique proposée par Daniel Martin et Frédéric-Paul Martin, pour qui cette criminalité *« recouvre l'ensemble des actes illégaux intéressant l'informatique et les télécommunications tant sur le plan des matériels que des logiciels »*[58]. Le cybercrime est une forme particulière de la criminalité informatique, forme qui ne s'exprime que sur et à travers le réseau, contrairement aux autres délits informatiques qui ne nécessitent pas d'interaction avec le réseau (ex : le piratage de CD).

Cette définition nous paraissant trop générale, nous avons cherché une définition plus précise de la criminalité informatique.

La complexité de ce type de criminalité s'est alors présentée, les différents auteurs utilisant chacun leur propre définition. Collard fait d'ailleurs remarquer qu'aucune définition n'est acceptée de manière générale, unique[59].

Ainsi, Don Parker définit la criminalité informatique comme *« tout acte illicite nécessitant une connaissance spécialisée de l'informatique, au stade de la perpétration, de l'enquête de police ou des poursuites pénales»*[60]. Il s'agit de la définition adoptée par le ministère de la Justice des Etats-Unis.

Cette définition ne nous semble pas pertinente. Ainsi, comme nous le verrons, la criminalité informatique ne nécessite pas une connaissance spécialisée de l'informatique, Parker parlant lui-même de criminels informatiques « amateurs »[61].

Pour Grabosky, directeur de recherches à l'Institut australien de Criminologie, *« la criminalité informatique recouvre les illégalités impliquant des systèmes informatiques comme instruments ou cibles des infractions »*[62].

---

[58] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 13.

[59] I., COLLARD, « Criminalité informatique en Belgique : hier les ténèbres. Demain…. », Rev. Ubiquité, novembre 98, n°1, p. 68.

[60] D.-B., PARKER, *Combattre la criminalité informatique*, Paris, Oros, 1985, p.18

[61] Nous analyserons ce point plus en détails dans la partie consacrée aux profils et aux motivations des hackers.

[62] P., GRABOSKY, « Computer crime in a bordeless world », Annales internationales de criminologie, 2000, vol. XXXVIII, n°1/2, pp. 67.

Pour l'O.C.D.E., *« l'abus informatique est tout comportement illégal, contraire à l'éthique ou non autorisé, qui concerne un traitement automatique et/ou une transmission de données »*[63].

Ces deux définitions nous semblent trop générales, trop vagues pour constituer des définitions « officielles », de référence. En effet, si l'on s'en réfère, par exemple, à la définition proposée par l'O.C.D.E., un acte immoral ou asocial, et donc contraire à l'éthique, pourrait être considéré comme relevant de la criminalité informatique, même s'il ne constitue pas une infraction pénale, pour peu qu'il concerne un système informatique ou de télécommunications[64].

Chez nos voisins allemands, la définition la plus utilisée est celle du groupe de travail qui réunit les chefs des services d'enquête criminelle des Etats allemands et l'Office fédéral des enquêtes criminelles : *« la criminalité informatique englobe tous les phénomènes dans le cadre desquels le traitement électronique des données est le moyen et/ou fait l'objet d'un acte donnant des raisons de soupçonner une infraction pénale »*[65].

Cette définition ne nous convient pas non plus, car elle définit la criminalité informatique sur base de faits qui ne sont pas avérés, sur lesquels porteraient simplement des soupçons.

A notre sens, c'est la définition de Daniel Martin qui cerne le mieux le concept de criminalité informatique. Il la définit comme étant «*« toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du délit ; tout délit dont le moyen ou le but est d'influencer la fonction de l'ordinateur ; tout acte intentionnel, associé d'une manière ou d'une autre à la technique informatique, dans laquelle une victime a subi ou aurait pu subir un préjudice et dans laquelle l'auteur a tiré ou aurait pu tirer un profit »*[66].

Elle regroupe les principales caractéristiques des actes de criminalité informatique (l'utilisation de l'ordinateur comme objet ou comme instrument de l'infraction, la technique informatique, la notion de profit) et nous semble donc donner un meilleur aperçu de ce que ce concept recouvre.

Nous ne trouvons pas en Belgique de définition « officielle ». Le gouvernement belge s'est abstenu de définir la criminalité informatique, avec comme souci d'éviter que les concepts soient trop rapidement dépassés, estimant que la terminologie doit rester neutre pour être évolutive[67].

Le législateur détermine néanmoins deux types de criminalité informatique : l'informatique comme moyen de perpétrer l'infraction et l'informatique comme but de l'infraction.

---

[63] Voy. W., SCHREIBER, « La délinquance assistée par ordinateur », R.I.P.C., 1997,51e année, n°464, p. 9.
[64] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 612.
[65] Voy. W., SCHREIBER, « La délinquance assistée par ordinateur », R.I.P.C., 1997,51e année, n°464, p. 9.
[66] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 13.
[67] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 9.

Si cette distinction est aisément compréhensible[68], il nous semble qu'il aurait été utile de poser un cadre général, déterminant la place de la criminalité informatique au sein de la « criminalité en général ».

Sur ce dernier point, la criminalité informatique est généralement considérée comme une sous-catégorie de la criminalité en «col blanc »[69]. Attardons-nous quelques instants sur les similitudes existant entre ces deux types de criminalité.

[68] Voir infra la partie consacrée à cette distinction.

[69] P., GLINEUR, *Droit et éthique de l'informatique*, Bruxelles, Story scientia, A la rencontre du droit, 1991, p. 180

B. SIMILITUDES ET DIFFÉRENCES ENTRE CRIMINALITÉ INFORMATIQUE ET CRIMINALITÉ EN COL BLANC

Dans cette partie, nous allons aborder les similitudes existant entre, d'une part la criminalité informatique et d'autre part la criminalité d'affaires, appelée également criminalité « en col blanc ».

Le droit pénal des affaires est défini par Mireille Delmasmarty, professeur à l'université de Paris I, comme étant *« la branche du droit pénal qui sanctionne, d'une part, les atteintes à l'ordre financier, économique, social et à la qualité de la vie ; d'autre part, les atteintes à la propriété, foi publique, intégrité physique des personnes, lorsque l'auteur a agi dans le cadre d'une entreprise, soit pour le compte de celle-ci, soit pour son compte propre si le mécanisme de l'infraction est lié à l'existence de pouvoirs de décision essentielle à la vie de l'entreprise »*[70].

Szabo, quant à lui, définit le crime d'affaires comme étant *« un acte illégal perpétré sans le recours à la contrainte physique, usant de la dissimulation et ayant une intention frauduleuse, en vue de l'obtention de propriétés ou d'avantages monétaires, ou pour éviter des pertes d'argent ou de propriétés par le truchement d'avantages obtenus dans les affaires ou à titre personnel »*[71].

Les similitudes avec la criminalité informatique apparaissent clairement, certains considérant même celle-ci comme une sous-catégorie de la criminalité en col blanc[72].

Tout d'abord, elles visent toutes deux un avantage financier, économique (bien que, comme nous le verrons, la criminalité informatique ne poursuit pas exclusivement ce type de buts).

Ensuite, tout comme la criminalité en col blanc, la criminalité informatique ne nécessite pas le recours à la contrainte physique, le hacker se servant uniquement de son ordinateur pour commettre son infraction.

Enfin, ces deux types de criminalité nécessitent également que les malfaiteurs ne soient pas de « simples » criminels, ayant des connaissances spécifiques, comme la fiscalité, la comptabilité ou encore, évidemment, la maîtrise de l'informatique.

De même, ces crimes sont plus complexes, dans leurs mécanismes comme dans leurs conséquences, rendant ces types de criminalité particulièrement difficiles à mesurer avec exactitude. Ces difficultés s'expliquent par différentes raisons (qui seront analysées dans le point suivant), comme le fait que ces infractions, relatives à la criminalité d'affaires comme à la criminalité informatique, ne font pas systématiquement l'objet de plaintes, les entreprises préférant généralement ne pas ébruiter leurs mésaventures afin de conserver une image rassurante pour leurs investisseurs et clients.

---

[70] DELMAS-MARTY, M., *Droit pénal des affaires*, 3e éd., t.1, Paris, PUF, 1990, pp. 8 et 9

[71] D., SZABO, « La criminalité d'affaires : aspects criminologiques », L'années sociologique, Presses Universitaires de France, 1981, p. 290.

[72] P., GLINEUR, *Droit et éthique de l'informatique*, Bruxelles, Story scientia, A la rencontre du droit, 1991, p. 180

A contrario, nous observons un certain nombre de différences non négligeables entre la criminalité informatique et celle en col blanc.

En effet, les criminels informatiques ne constituent pas une catégorie de criminels comme les autres, étant les seuls à publier des livres, des lettres d'information et se réunissant en congrès publics (le Congrès DefCon dont nous parlerons plus tard)[73].

Ainsi, si la criminalité en col blanc vise exclusivement des objectifs d'ordre économique, la criminalité informatique poursuit également d'autres buts, à caractère politique par exemple (comme le cyberterrorisme et l'hacktivisme qui seront analysés plus tard), et s'éloigne donc, dans certains cas, de la criminalité d'affaires telle qu'elle vient d'être définie.

De plus, si la criminalité d'affaires concerne le monde de l'entreprise, la criminalité informatique menace également les particuliers, voire même les états.

En conclusion, si la criminalité informatique peut effectivement être rapprochée de la criminalité en col blanc, il ne nous semble pas pour autant qu'elle puisse être considérée à proprement parler comme une sous-catégorie de celle-ci.

En effet, si elle présente des interactions, des connexions avec la criminalité en col blanc, il n'en reste pas moins que certains crimes informatiques ne rentrent pas dans cette catégorie.

Il nous semble donc qu'il faudrait considérer la criminalité informatique comme une catégorie à part entière, les différentes formes de crimes informatiques que sont le hacking, l'hacktivisme ou encore les infractions relatives au racisme et à la xénophobie sur Internet poursuivant des objectifs trop variés que pour lui permettre d'être inclue dans un ensemble plus grand comme la criminalité d'affaires.

---

[73] B., STERLING, *The Hacker crackdown, Law and Disorder on the Electronic*, New York, Frontier Bantam Books, 1992, p.173.

Section 2 – L'étendue du phénomène

Comme nous venons de le voir, la criminalité informatique se caractérise notamment par un certain flou concernant son ampleur et l'étendue exacte des dégâts qu'elle peut causer.

Comme n'importe quel phénomène criminel, une représentation parfaitement exacte de son ampleur est utopique.

Si différentes actions ont été mises en place afin de mesurer l'ampleur du phénomène, nous allons voir que les résultats sont souvent sujets à caution (statistiques policières, sondages et enquêtes) ; que les organismes ne suivent pas toujours une méthodologie correcte, utilisant parfois des méthodes illégales (c'est par exemple le cas de la BSA) ; et que sur le plan international, les recherches n'en sont encore qu'au stade embryonnaire (comme nous le confirmera un peu plus tard, l'analyse du cybercriministstitut).

Il doit être souligné que, par souci de concision, nous n'avons abordé que les sources d'information les plus répandues et les plus utilisées.

A. LES PRINCIPALES SOURCES D'INFORMATION SUR LA CRIMINALITÉ INFORMATIQUE

1) Au niveau national

a) Les statistiques policières

Les services de police se trouvent de plus en plus confrontés à la délinquance informatique. Des structures, comme l'actuelle Computer Crime Unit ou l'ancienne BOGO-Team par exemple, ont d'ailleurs été spécifiquement créées afin de lutter contre ce type de crimes.

Il faut d'ailleurs pointer le fait que, bien que leur fonction principale devrait être la lutte contre le crime de nature informatique, ces services passent le plus clair de leur temps à s'occuper de faits mineurs, n'ayant bien souvent qu'un très faible rapport avec l'informatique (comme l'envoi de SMS d'insultes par exemple) [74].

Dès lors, lorsque l'on analyse les statistiques policières relatives à la criminalité informatique, il faut bien avoir conscience que cette catégorie regroupe de nombreux autres faits que ceux visés par la loi du 28 novembre 2000.

[74] Nous y reviendrons plus tard dans la partie consacrée à l'analyse de l'activité policière.

Outre cette première mise en garde, d'autres critiques doivent venir tempérer les résultats obtenus.

D'une part, les inexactitudes qu'ils peuvent présenter, en raison des erreurs involontaires d'encodage, les différences d'appréciation entre services, entre enquêteurs.

D'autre part, les statistiques criminelles peuvent avoir un effet déformant en raison du fait qu'elles placent les crimes et les délits sur le même plan. Il ne sera, par exemple, pas fait de différence entre la modification d'un site Internet et l'utilisation d'une fausse carte de crédit : les deux infractions seront considérées comme des faux en informatique.

De même, si la mesure du crime informatique à un instant donné est délicate, la mesure de l'évolution de cette criminalité (comme n'importe quel type de criminalité) l'est tout autant. En effet, constater l'augmentation du nombre de crimes peut donner lieu à plusieurs interprétations : soit les délinquants sont plus nombreux, soit ils sont plus actifs, soit il y a plus d'opportunités,…

Enfin, comme nous le verrons avec l'étude du chiffre noir, la criminalité informatique est un des domaines les plus mal estimés, en raison de ses caractéristiques propres (atteinte à la réputation des entreprises, crainte de dégâts plus importants en cas de dénonciation, nécessité d'une protection optimale et coûteuse,…).

b) Sondages et enquêtes

Les sondages et enquêtes ne sont pas toujours les méthodes les plus aisées afin de récolter des informations sur le coût de la criminalité informatique.

Si elles peuvent fournir sans trop de réticences des renseignements sur les méthodes de piratage utilisées, les victimes sont souvent beaucoup plus discrètes sur l'importance des dégâts causés.

Les raisons sont multiples et propre à la criminalité informatique, comme nous le verrons avec l'analyse du chiffre noir.

Les méthodes de sondages et d'enquêtes comportent également différents biais, qu'il nous faut avoir à l'esprit lors de l'analyse de chiffres.

Ces biais peuvent venir du mode de recueil des informations (questionnaires, enquêtes téléphoniques, ….), du type d'informations recherchées, et surtout des personnes interrogées et des sondeurs.

Concernant ce dernier point, nous proposons l'analyse de la Business Software Alliance et de ses méthodes.

c) La Business Software Alliance

La Business Software Alliance (BSA)[75] fournit de nombreuses informations, principalement sur le piratage de logiciels. Mais, comme nous allons le voir, ces informations sont à prendre avec précaution.

« Business Software Alliance (BSA) est l'organisation la plus en vue engagée à promouvoir un univers en ligne sécuritaire et respectueux des lois.

Nous sommes les porte-paroles, sur le marché international, devant les gouvernements et avec les consommateurs, des secteurs des logiciels, du matériel et des technologies pour Internet. Les membres de BSA représentent les industries les plus dynamiques du monde.

BSA informe les utilisateurs d'informatique des droits d'auteur de logiciels et de la sécurité sur Internet ; se fait le champion des politiques de l'état encourageant l'innovation et développant les opportunités commerciales; et lutte contre le piratage des logiciels. Établie en 1988, BSA a des programmes dans 65 pays répartis dans le monde entier»[76].

Si la BSA est pratiquement la seule organisation, en Belgique, luttant avec plus ou moins d'efficacité contre le piratage de logiciels, elle n'est pas à proprement parler « respectueuse des lois », allant parfois jusqu'à inciter à la délation.

De ce fait, la BSA, qui est surtout un groupe de pression regroupant les principaux éditeurs de logiciels américains, vient encore de se voir critiquer. Cette fois, c'est l'association des experts-comptables britanniques (Acca) qui dénonce ses méthodes en matière de lutte contre le piratage. La BSA UK a ainsi envoyé un courrier à 80 000 PME anglaises, avec des formules menaçantes qui laissaient croire que les destinataires étaient obligés de répondre[77]. De même, la BSA a fait l'objet en France, d'une véritable levée de bouclier par le Clusif devant ses méthodes [78], sans que cela semble influer sur son comportement.

Relativement coutumière de ce type de pratiques, la BSA a d'ailleurs déjà été condamnée en Belgique. Dans leur jugement, les magistrats belges soulignent la *« perversité »* de la dernière campagne de la Business Software Alliance. Les éditeurs avaient publié dans la presse des annonces titrées : *« C'est un voleur. Et un hypocrite. Et ça lui est bien égal. Des gens comme ça on en trouve partout. Du genre à se croire plus malin que les autres, […] les mêmes qui montent sur leurs grands chevaux quand leurs clients ne paient pas en temps voulu. Mais tel est pris qui*

---

[75] Cette organisation est active dans plusieurs pays, mais nous n'envisagerons principalement ici que son activité en Belgique.
[76] BSA, www.bsa.org.
[77] Le Monde, www.weblmi.fr. (Nous ne donnerons pas de référence précise quant aux articles extraits su sites Internet du Monde informatique, car ceux-ci changent constamment d'adresse au sein de celui-ci).
[78] X, « Le commentaire du Clusif à propos de la campagne BSA », Logiciels & Systèmes, 1999, mars 1999, n°36. (consultable à l'adresse http://www.grd-publications.com/art/ls036/ls036058.htm).

croyait prendre. Car avec votre aide, ils peuvent se faire prendre. Et ce jour-là, leur logiciel va leur coûter cher, très cher : les amendes sont lourdes et ils risquent même la prison [...] Dès que nous aurons de vos nouvelles, ils auront des nôtres». Neuf sociétés ont porté plainte, parmi lesquelles *Sema Group* et *l'Acodit*, une association de revendeurs. Les juges ont tranché : *« Une telle méthode n'est pas neuve et a fait la preuve de sa perversité, à une toute autre échelle il est vrai, dans un passé qui n'est pas si lointain et dont l'enseignement commande de qualifier de contraire aux bonnes mœurs dans la moindre de ses applications»*[79].

2) Au niveau international

a) Nécessité d'une recherche criminologique internationale

La recherche criminologique dans le domaine de la criminalité informatique est une nécessité absolue. Seule une connaissance précise des changements, développements survenant dans les manifestations et les caractéristiques de la délinquance informatique permettra le développement de systèmes de sécurité préventifs, l'élaboration de réformes législatives et une répression judiciaire efficaces.

Cette recherche criminologique doit être effectuée en étroite coopération internationale[80]. La délinquance informatique existe non seulement dans tous les pays, mais tend surtout à être un problème international et transnational, nécessitant donc que les législateurs des différents pays s'attaquent au problème, ce qui suppose donc qu'ils en aient une bonne connaissance.

Dès lors, cette coopération internationale doit être basée sur une classification des cas de criminalité informatique selon des critères de différenciation uniformes et une méthode commune de collecte des données, afin d'éviter les écueils décrits précédemment et d'obtenir une représentation plus proche de la réalité de l'ampleur du phénomène de la criminalité informatique.

C'est dans cette optique qu'a été mis sur pied le Cybercriminstitut.

---

[79] Comm. Bruxelles, 27 novembre 1997, *R.D.C.*, 1998, pp. 326 à 332.
[80] Ceci, entre autres, en raison de l'absence de frontières « réelles » du réseau Internet.

b) Le Cybercriminstitut

Sous la forme d'une association à but non lucratif, plusieurs personnes issues de milieux différents (universitaires, diplomates, chefs d'entreprise, juristes, fonctionnaires,….) se sont regroupées afin de créer l'Institut international des hautes études de la Cybercriminalité[81].

Il s'agit d'accueillir au sein *« d'un institut largement ouvert sur le plan international »*[82] tous les milieux concernés (états, multinationales, entreprises publiques, privées, commerciaux, particuliers,…) afin[83] :

- d'accroître la connaissance de la criminalité de haute technologie mettant en cause les Nouvelles technologies de l'Information et de la Communication (NTIC), et ce, tant sur le plan national qu'international, et sous une approche pluridisciplinaire : juridique, criminologique, sociale, culturelle, économique,…. ;
- d'apporter des propositions concrètes visant à créer ou renforcer les moyens de lutte contre la criminalité informatique, au niveau gouvernemental ou privé ;
- de permettre, sur le plan national comme sur le plan international, l'établissement d'un dialogue entre toutes les parties concernées, en vue de l'élaboration de parades communes ;
- de développer une activité d'analyses, de recherches, de documentation, de voyages d'études, d'échanges,… afin de favoriser l'établissement d'un courant d'informations ;
- de constituer un lieu de rencontre entre acteurs et observateurs impliqués dans le domaine ;
- de mettre *« les NTIC au service de l'Homme en prévenant la prolifération des sanctuaires informatiques, refuges des criminels et en luttant notamment contre le blanchiment d'argent et la corruption qu'ils engendrent »*[84]

Le Cybercriminstitut fonctionne principalement par commissions où chacun peut s'inscrire et participer[85], les sujets abordés lors de ces commissions étant variés (droits de l'Homme et protection des libertés, sécurité des entreprises, évaluation de menaces,…).

Des réunions de commissions périodiques, des forums de discussions,… sont établis et la publication de plusieurs ouvrages est également prévue.

---

[81] Cybercriminstitut, www.cybercriminstitut.com.
[82] Cybercriminstitut, www.cybercriminstitut.com.
[83] Nous ne citerons ici que les principaux objectifs de l'Institut. Nous renvoyons sur son site Internet pour de plus amples renseignements (www.cybercriminstitut.com).
[84] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 191.
[85] En ce compris les particuliers, pour peu qu'ils marquent un certain intérêt et une certaine connaissance de la criminalité informatique.

Enfin, un congrès annuel regroupant les adhérents et les médias autour de sujet d'actualités relatifs aux nouvelles technologies est également organisé, le premier congrès s'étant tenu en novembre 2001.

L'ambition de l'Institut est de compter dans le paysage des NTIC et de devenir une ONG reconnue et entendue au niveau international.

Il est encore trop tôt pour dire si les objectifs de l'Institut seront remplis et de quelle manière. Néanmoins, il traduit la prise de conscience d'une criminalité informatique internationale et mal perçue.

L'implication de milieux divers dans les propositions présentées, ainsi que dans les différentes commissions, devrait également contribuer à circonscrire les différentes composantes de la criminalité informatique.

Il sera intéressant de voir dans quelle mesure les propositions envisagées seront suivies par les états notamment, et si l'Institut pourra jouer un rôle véritablement fédérateur.

A suivre donc…

B. LE CHIFFRE NOIR

Au niveau mondial, seules quelques recherches empiriques fournissent un résultat fiable. La comparaison entre ces différentes recherches est difficile : différences entre les définitions des infractions observées, différences dans les méthodes de sélection et de vérification utilisées,… Ce qui explique que le nombre de délits informatiques «parfaitement vérifiables » recensés par toutes les études empiriques soit peu élevé[86].

Ainsi, par exemple, la Commission des Communautés Européennes en 1983 avait commandité une étude internationale sur les cas de dommages liés à l'informatique ayant lieu en Belgique, France, Allemagne de l'Ouest, Italie et Royaume Uni depuis 1979. Cette étude n'a enregistré que 260 cas. De prime abord, ce faible chiffre pourrait s'expliquer par le fait qu'au début des années 1980 ce type de criminalité n'était pas très répandu, mais lorsque l'on sait que sont compris, dans ces 260 cas, les dommages accidentels, on se rend compte que ce chiffre devient «trop » faible pour représenter correctement la réalité (environ 50 cas par an pour l'ensemble des pays cités).

Le nombre de délits informatiques vérifiables ne permet donc pas de tirer des conclusions quant au nombre de cas réels, les cas non détectés étant sans doute beaucoup plus nombreux.

Cette supposition est basée sur plusieurs constatations.

- Tout d'abord sur le fait qu'il existe des difficultés spécifiques concernant la détection et la preuve des délits informatiques. En effet, comme nous l'avons vu, lorsqu'une panne informatique se produit, diverses causes peuvent l'expliquer, comme les risques naturels, l'erreur humaine ou la malveillance ; mais la preuve de la malveillance ne sera pas facile à obtenir, les pirates effaçant généralement toute trace de leur intrusion.

- Un grand nombre de délits découverts ne sont pas signalés par les entreprises et font l'objet de procédures disciplinaires internes, les entreprises craignant de porter atteinte à leur réputation et à la confiance des investisseurs, actionnaires, clients,…

- Les cas portés devant les autorités judiciaires ne sont pas toujours poursuivis, en raison de leur manque de spécialisation et de l'absence de moyens financiers.

- D'une manière générale, le manque de visibilité de cette délinquance[87].

---

[86] U., SIEBER, *La délinquance informatique*, Bruxelles, Story scientia, Précis et travaux de la Faculté de droit de Namur, n°9, 1990, p. 39.

[87] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p. 19.

- L'absence d'obligation pour les victimes de porter plainte en vue d'obtenir réparation du préjudice par les compagnies d'assurances, contrairement à la pratique en matière de cambriolage par exemple.

Un autre point venant appuyer cette supposition d'une grande différence entre le nombre de cas enregistrés et le nombre de cas réels provient de la comparaison entre pays.

Prenons l'exemple de la France et des Etats-Unis. Les écarts obtenus sont tellement importants (toutes proportions gardées) qu'on ne peut qu'en conclure que ce phénomène n'est pas correctement perçu. Ainsi, face aux 719 infractions recensées par la PJ en France pour l'année 1999, le site IFCC (Internet Fraud Complaint Center) du FBI a enregistré 19490 plaintes entre le 8 mai et le 3 novembre 2000 !

Plusieurs explications permettent de comprendre cette différence. Tout d'abord, il y a, comme nous l'avons vu dans la partie consacrée au réseau Internet, beaucoup plus d'internautes aux Etats-Unis, la culture Internet étant moins développée en France. De plus, les chiffres de la PJ française représentent les plaintes enregistrées de personnes identifiées, alors que celles portées sur le site du FBI peuvent être faites de manière anonyme. Cette méthode peut être avantageuse pour les entreprises connues victimes de crimes informatiques, mais également désavantageuse, ces plaintes pouvant être le fait de personnes se croyant victimes de malveillance alors que ce n'est pas la cas ou encore de farceurs. Enfin, d'une manière générale, les méthodes de recueil de données ne sont pas standardisées sur le plan international.

Il n'en reste, après avoir pris en compte ces éléments, que la différence entre ces deux pays est énorme, surtout si on l'on s'en réfère aux périodes observées (719 cas pour 12 mois en France contre 19490 cas pour 6 mois aux Etats-Unis). Dès lors, nous posons l'hypothèse selon laquelle les plaignants identifiés (aux Etats-Unis et en France) ne sont que la partie émergée de l'iceberg, les méthodes de recueil étant beaucoup trop disparates et peu fiables que pour donner une représentation exacte de l'ampleur de la criminalité informatique.

Compte tenu des considérations qui viennent d'être développées, il semble évident que si l'on veut avoir des statistiques « relativement » fiables, un autre mécanisme de dépôt de plainte doit être envisagé. Le Cybercriminstitut propose ainsi d'utiliser Internet et un réservoir général préservant l'anonymat pour évaluer d'une manière objective et internationale ce sujet.

Nous pointons quant à nous les risques que ce type de méthode peut amener quant à la fiabilité des plaintes reçues (comme c'est le cas pour l' Internet Fraud Complaint Center du FBI), mais soulignons néanmoins la volonté et la prise de conscience de l'utilité d'avoir des statistiques fiables.

Section 3 – Le coût de la criminalité informatique

Les diverses enquêtes internationales sur la délinquance informatique avancent des montants de dommages variables, vraisemblablement en raison de l'utilisation de techniques de déclarations différentes selon les pays[88].

Il y a néanmoins un point sur lequel toutes ces études s'accordent : les dommages causés par la criminalité informatique sont beaucoup plus importants que ceux causés par la délinquance « traditionnelle ».

Ainsi, l'Institut américain sur la sécurité informatique (Computer Security Institute[89]) et le FBI (Federal bureau of investigation) viennent de rendre public le *« rapport 2001 sur les crimes informatiques et la sécurité »*.

Si les auteurs du rapport ont interrogé 538 entreprises, organisations gouvernementales et universités américaines, seulement 35% des personnes interrogées ont accepté de divulguer les chiffres de leurs pertes, ce qui n'est pas étonnant, la discrétion concernant les pertes liées à la criminalité informatique étant, comme nous l'avons vu, assez caractéristique des victimes d'actes de piratage. Il apparaît néanmoins que les pertes de celles-ci s'élèvent à plus de 455 millions de dollars pour l'an 2001, pertes qui ne seraient donc que la partie émergée de l'iceberg[90] !

Internet est désigné maillon le plus faible du système d'information par près de 70% des entreprises. Au total, 94 % ont eu à subir une attaque virale courant 2001 - plus qu'en Europe si l'on compare à l' étude IDC[91] où plus des trois quarts des entreprises européennes interrogées reconnaissent avoir souffert de virus[92] - 40 % une intrusion et 38 % ont subi une attaque par saturation.

A cela, il faut ajouter que depuis l'an 2000, les attaques de sécurité dans le monde auraient coûté en temps perdu 1.600 milliards de dollars aux entreprises, selon le sondage annuel réalisé par InformationWeek Research et le cabinet de conseil PriceWaterhouseCoopers. D'après la firme Reality Research and Consulting, les sociétés du seul continent nord-américain auraient globalement retranché de leur productivité 6.822 personnes pendant 365 jours.

Autre chiffre intéressant, sur 4.900 décideurs généraux et informatiques responsables de la sécurité interrogés dans le monde, près de 70% considéreraient la sécurité informatique comme une

---

[88] Les qualifications juridiques peuvent être différentes d'un pays à l'autre, certaines infractions peuvent être englobées dans le droit pénal commun dans un pays, et constituer une infraction « informatique » à part entière dans un autre,…

[89] The Computer Security Insitute, www.gocsi.com.

[90] X, « La criminalité informatique coûte des milliards de dollars par an », Journal Le Soir, 13 avril 2002.

[91] IDC est le premier groupe mondial de conseil et d'étude sur les marchés des technologies de l'information. La structure conseil du groupe forme un réseau international de 770 consultants répartis dans plus de 42 pays. Le site de ce groupe est consultable à l'adresse www.idc.fr.

[92] Le Monde, www.weblmi.fr.

priorité. Cependant, les budgets[93] consacrés restent à un niveau très bas, en dessous de 50.000 dollars pour la moitié des personnes interrogées[94].

Les montants astronomiques des dommages causés par la délinquance informatique sont aisément compréhensibles au regard de la valeur importante des données stockées dans les systèmes.

Ainsi, en matière d'escroquerie par exemple le pirate informatique, pour un investissement minimum (un ordinateur et une ligne téléphonique) peut obtenir un gain très important.

En matière d'espionnage informatique, la même règle s'applique, pour peu que l'on puisse aisément quantifier la valeur de ce type d'informations.

Sachant que n'importe qui peut potentiellement être un pirate informatique, quel est le budget que devront prévoir les particuliers, les entreprises, les multinationales, les états, afin de se protéger correctement?

Nous serions tentés de dire que la réponse variera en fonction des intérêts à protéger. Néanmoins, cette supposition n'est pas de mise à l'analyse des budgets débloqués[95]. Les cibles potentielles (dans leur ensemble) sont en général trop sûres d'elles, n'imaginant pas que leur système puisse être violé. Pourtant, une seule règle compte dans ce type de démarche, illustré par le slogan favori des hackers, au parfum de menaces : *« Ce qui est fait par l'homme peut également être défait par l'homme »*[96].

En résumé, le coût du crime informatique est la somme de trois composantes :

- Le coût des pertes directes (ex : transferts de comptes frauduleux)
- Les coûts des opérations de protection (ex : consultance, logiciels, matériel,…)
- Les pertes financières indirectes dues au temps perdu à remettre le système en place et à réparer les dégâts (ex : chômage technique, remplacement du matériel, perte de compétitivité,…).

---

[93] Le budget comprend ici le matériel, les logiciels, le conseil en amont et les salariés.
[94] Le Monde, www.weblmi.fr.
[95] Cf. supra.
[96] Nous pouvons retrouver ce type de déclaration sur la majorité des forums de discussions de hackers. Lorsqu'un pirate demande de l'aide, ou se trouve en difficulté devant un nouveau type de protection, ce slogan est utilisé afin de motiver la communauté des hackers à trouver la faille dans le logiciel, dans le système attaqué.

Section 4 – Conclusion

Les éléments qui viennent d'être exposé portent déjà en eux le germe d'une explication quant aux raisons sous-tendant l'élaboration de la nouvelle loi sur la criminalité informatique de novembre 2000.

Si les difficultés sont multiples, les tentatives pour y remédier le sont tout autant.

Devant la difficulté posée par la définition de la notion de criminalité informatique, le législateur a choisi de ne pas la définir du tout. Si cette position peut se comprendre – la raison première étant la volonté de rester le plus large possible pour être applicable aux progrès technologiques à venir -, il nous semble qu'une définition n'aurait pas été superflue. Il est en effet assez paradoxal de légiférer par rapport à une matière qui n'est pas clairement définie. Nous y reviendrons plus tard.

Ensuite, quand aux similitudes avec la criminalité en col blanc avancées par plusieurs auteurs, nous sommes, quant à nous, plutôt partisans de la prépondérance de leurs différences. Certains actes constitutifs de la criminalité informatique, comme le cyberterrorisme par exemple, ne rentrant pas dans la définition de la criminalité en col blanc, nous ne voyons aucune raison de faire de la criminalité informatique une sous-catégorie de celle-ci.

L'étendue du phénomène nécessite elle aussi d'être déterminée de manière fiable, afin que la lutte contre la criminalité informatique soit efficace. Il s'agit là d'une condition essentielle à une évaluation claire et raisonnable des objectifs, moyens et possibilités de la lutte contre la criminalité informatique.

A ce titre, des initiatives comme la création du Cybercriminstitut, en plus d'être l'expression d'une prise de conscience de la nécessité d'une recherche criminologique au niveau internationale, nous semblent particulièrement appropriées, tout en soulignant que certaines règles méthodologiques devront être clairement définies, à peine de retomber dans les erreurs que l'on tente de corriger…

Titre IV – Le respect de la vie privée confronté aux nouvelles technologies

La question du respect de la vie privée dans le domaine des nouvelles technologies nous semble devoir être entendue selon deux acceptions.

Tout d'abord, il nous paraît essentiel de pointer que lorsqu'un pirate s'infiltre sur un ordinateur, quelque soit sa motivation, il viole l'intégrité de celui-ci. Etant entendu que l'ordinateur, devient de nos jours un lieu d'exercice de l'activité privée et professionnelle de l'individu[97], celui-ci peut être considéré comme un *« domicile informatique »*[98] .

Dès lors, le statut d'inviolabilité octroyé par l'article 15 de la Constitution nous semble devoir lui être accordé.

De même, l'utilisateur a droit au respect de sa vie privée, en vertu, entre autres, de l'article 22 de la Constitution[99].

Si ces considérations peuvent paraître évidentes, elles n'en ont pas moins une importance capitale dans le domaine de l'informatique, qui sera abordée plus tard, dans la partie consacrée à l'analyse de la loi du 28 novembre 2000 relative à la criminalité informatique.

Ensuite, il est un deuxième domaine où les informations relatives à la vie privée risquent de souffrir de leur confrontation aux nouvelles technologies, à savoir le traitement des données à caractère personnel.

De nombreuses institutions (hôpitaux, institutions publiques, bancaires,…) sont connectées à un ou des réseaux, internes ou externes (comme Internet). Celles-ci ont, pour la plupart, des bases de données reprenant leurs affiliés, clients et autres patients, si bien que ceux-ci encourent un risque potentiel plus important de voir leurs données personnelles être au mieux consultées, ou au pire détruites, et ce par n'importe qui (ou presque). Plus important car si ce risque est tout à fait présent au sein même de l'institution et par le seul fait de l'intervention humaine[100], celui-ci est multiplié dès la connexion au réseau Internet. Ce ne seront plus seulement quelques dizaines d'employés qui auront accès à vos données, mais des centaines de millions de personnes. Du moins potentiellement, étant bien entendu que la majorité des internautes ne sont pas tous des pirates informatiques.

---

[97] H.D., BOSLY, D., VANDERMEERSCH, *Droit de la procédure pénale*, Brugge, La Charte, 1999, p. 308

[98] *Rapport explicatif de la Recommandation R(89) 9 du Conseil de l'Europe*, éd. du Conseil de l'Europe, Strasbourg, 1990, p. 56.

[99] Ce droit est également garanti par la Déclaration universelle des droits de l'homme et la Convention européenne des droits de l'homme.

[100] Nous renvoyons ici au Titre I de la Première partie consacré aux risques.

De plus, le traitement de données à caractère personnel est réglé par toute une série de conditions relatives à la méthode de récolte de ces données, à l'utilisation qui en sera faite, par qui, etc. Précisons d'emblée que ces éléments, s'éloignant de notre sujet principal, ne seront pas abordés ici.

Bien que le respect de la vie privée soit un élément primordial de notre vie de tous les jours, il n'est pas spécifique à la criminalité informatique. Si notre vie privée peut se voir violer par l'intrusion d'un criminel informatique sur notre ordinateur, elle peut tout autant l'être par un voisin curieux épiant nos fenêtres. De même, avant de pouvoir être volées, modifiées, détruites par des pirates informatiques, les données personnelles se trouvant dans une quelconque base de données peuvent avant tout se voir interceptées par les administrateurs de cette même base de données.

Dès lors, et par souci de concision, ces matières ne seront développées que brièvement, nous limitant principalement, pour chacune des acceptions, à dresser l'arsenal législatif en vigueur. Nous nous permettons de renvoyer à l'abondante littérature consacrée à ces matières pour de plus amples explications[101].

Nous commencerons par citer les principaux textes, nationaux et internationaux garantissant le respect dû à la vie privée, étant entendu que des considérations relatives à cette notion émailleront l'ensemble de notre exposé, l'intrusion sur un ordinateur impliquant *ipso facto* la violation de la vie privée de son utilisateur.

Nous ferons ensuite de même pour le traitement des données à caractère personnel, abordant brièvement la commission de protection de la vie privée.

Nous terminerons cette partie par un large exposé sur le réseau Echelon. Celui est en effet l'exemple parfait d'un piratage informatique qui ne vise *que* la violation de la vie privée, puisqu'il a pour principal objectif de récolter et de décrypter l'ensemble des messages transitant par les moyens de télécommunications (fax, e-mails, …).

De plus, l'analyse de ce réseau nous paraît particulièrement intéressante pour notre sujet, étant donné que ce ne sont plus un particulier ou un groupe de particuliers qui violent les principes du secret des communications et de respect de la vie privée, mais bien des institutions étatiques !

---

[101] Voy. notamment Y., POULLET, « Internet et vie privée : entre risques et espoirs », J.T., 2001, pp. 155 à 164 ; Y., POULLET, E., DE TERWANGNE, P., TURNER, *Vie privée : nouveaux risques et enjeux*, Bruxelles, Story-scientia, Cahiers du Cahiers du Centre de Recherches Informatique et Droit, n°13, 1997 ; GOLVERS, L., « L'informatique et la protection de la vie privée », http://www.droit-technologies.org, 11 janvier 2001.

Section 1 – Le respect du droit à la vie privée

Comme nous venons de le préciser, nous ne nous bornerons ici à exposer les principaux textes garantissant le droit au respect de la vie privée.

La notion de vie privée semble être un concept si bien compris, si fondamental, qu'aucune législation, quel que soit le pays, ne présente de définition de celle-ci[102]. Mais ceci n'a pas empêché les instances nationales et internationales de légiférer en la matière.

A. AU NIVEAU INTERNATIONAL

1) La Déclaration universelle des droits de l'homme

La Déclaration universelle des droits de l'Homme[103], adoptée par l'Assemblée Générale des Nations Unies le 10 décembre 1948 à Paris, est le texte le plus fondamental concernant les droits de chacun en tant qu'Homme (et non seulement en tant que citoyen), si bien que chaque droit qui y est garanti se doit d'être ardemment défendu et protégé.

Le préambule de ce texte précise à ce titre que *« l'Assemblée Générale proclame la présente Déclaration Universelle des Droits de l'Homme comme l'idéal commun à atteindre par tous les peuples et toutes les nations afin que tous les individus et tous les organes de la société, ayant cette Déclaration constamment à l'esprit, s'efforcent, par l'enseignement et l'éducation, de développer le respect de ces droits et libertés et d'en assurer, par des mesures progressives d'ordre national et international, la reconnaissance et l'application universelles et effectives, tant parmi les populations des États Membres eux-mêmes que parmi celles des territoires placés sous leur juridiction ».*

Le droit à la vie privée est garanti par l'article 12 de la Déclaration qui expose que *« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».*

---

[102] L., GOLVERS, « L'informatique et la protection de la vie privée », http://www.droit-technologies.org., 11 janvier 2001.

[103] Déclaration universelle des droits de l'Homme, adoptée le 10 décembre 1948 par l'assemblée des Nations Unies, *M.B.*, 31 mars 1949, p. 2488.

2) La Convention européenne des Droits de l'Homme

S'inspirant de la Déclaration Universelle des Droits de l'Homme de 1948, le Conseil de l'Europe a adopté en 1950 la Convention Européenne des Droits de l'Homme, qui énonce divers droits, dont celui relatif au respect de la vie privée.

L'article 8 garantit ainsi le droit au respect de la vie privée et familiale :

1) Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et quelle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui[104].

B. AU NIVEAU NATIONAL

Au niveau national, nous trouvons principalement la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunication privées[105], et, bien entendu, la Constitution.

La Constitution belge a traduit ce droit au respect de la vie privée en son article 22 qui déclare que *« chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi »*[106].

L'inviolabilité du domicile est également garantie, l'article 15 précisant que *« le domicile est inviolable ; aucune visite domiciliaire ne peut avoir lieu que dans les cas prévus par la loi et dans la forme qu'elle prescrit »*[107].

Ces textes montrent bien que le respect de la vie privée est un principe fort, et que lorsque celui-ci devra s'incliner devant l'action des autorités, ce sera dans des cas légalement prévus.

---

[104] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et Protocole additionnel, signé à Paris le 20 mars 1952, approuvés par la loi du 13 mai 1955, *M.B.*,19 août 1955.
[105] L. du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunication privées, *M.B.*,10 mai 1995, p. 01542.
[106] Const., art. 22.
[107] Const., art. 15.

Section 2 – Le traitement des données à caractère personnel

Bien que les textes relatifs à la notion de respect de la vie privée qui viennent d'être décrits soient applicables, in fine, au traitement des données à caractère personnel, il existe néanmoins certains textes spécifiques à cette matière.

A. AU NIVEAU INTERNATIONAL

· Les lignes directrices de l'O.C.D.E.

Le 23 septembre 1980, l' Organisation de coopération et de développement économiques (O.C.D.E.) a publié des *« lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel »*. Bien qu'elle n'ait aucune valeur juridique contraignante, cette recommandation prévoit que les Etats doivent assurer trois types d'obligations :

- assurer la libre circulation des données ;
- respecter et protéger la vie privée et les libertés individuelles ;
- une obligation d'information et d'assistance mutuelle.

Ces lignes directrices ont été complétées en 1985 par une déclaration sur les flux transfrontières de données[108].

· Les lignes directrices des Nations Unies

Dans la résolution n°45-95 du 14 décembre 1990, l'Assemblée générale des Nations unies a adopté un certain nombre de lignes directrices. Celles-ci, sans avoir de valeur véritablement contraignante, sont plus étendues que celles de l'O.C.D.E., puisqu'elles concernent à la fois les fichiers publics et privés.

De plus, la notion de « données sensibles » est appréhendée plus largement, puisqu'il s'agira des *« données susceptibles de pouvoir donner lieu à des discriminations illicites ou arbitraires, incluant les informations sur les origines raciales ou ethniques, la couleur, la vie sexuelles, les opinions politiques, philosophiques ou autres telles que l'appartenance à un syndicat ou à une association »*[109].

---

[108] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 118 et suiv.

[109] Voy. D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 119 et suiv.

· L'Organisation internationale du travail

Le Bureau international du travail (BIT) a adopté en 1996 un recueil de directives pratiques à propos de la protection des données personnelles concernant les travailleurs. Le BIT estime que les données relatives à la vie sexuelle, les opinions politiques, religieuses ou autres ainsi que les condamnations pénales doivent être considérées comme des données sensibles.

Ce recueil n'a lui non plus aucune valeur contraignante[110].

· L'Organisation mondiale du commerce

L'Organisation mondiale du Commerce a édicté une série de dispositions, qui bien que ne s'intéressant qu'indirectement à la protection de la vie privée, peuvent malgré tout s'y rattacher. C'est ainsi le cas de l'article XIV de l'accord du 15 avril 1994 qui dispose que *« sous réserve que ces mesures ne soient pas appliquées de façon à constituer soit un moyen de discrimination arbitraire ou injustifiable entre les pays où des conditions similaires existent, soit une restriction déguisée au commerce des services, aucune disposition du présent accord ne sera interprétée comme empêchant l'adoption ou l'application à tous les membres de mesures (…) nécessaires pour assurer le respect des lois et règlements qui ne sont pas incompatibles avec les dispositions du présent accord, y compris celles qui se rapportent (…) à la protection de la vie privée des personnes pour ce qui est du traitement et de la dissémination de données personnelles, ainsi qu'à la protection du caractère confidentiel des dossiers et comptes personnels »*[111].

Bien que cette dernière disposition n'ait pas non plus de véritable effet contraignant, il est intéressant de constater que la plupart des organisations internationales essaient d'assurer une protection minimale des données personnelles.

---

[110] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, 119 et suiv.

[111] Voy. D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 120 et suiv.

B. AU NIVEAU EUROPÉEN

Dès le début des années 60, avec les progrès réalisés dans le domaine du traitement électronique des données et l'apparition des premiers gros ordinateurs et, par voie de conséquence, la tendance manifeste à l'enregistrement électronique massif de données concernant la vie privée des particuliers, le Conseil de l'Europe s'est retrouvé face à l'obligation d'établir un cadre de principes et de normes spécifiques afin d'éviter la collecte et le traitement déloyaux de données à caractère personnel.

Un premier pas a été fait en 1973 et 1974 avec l'adoption des Résolutions (73) 22 et (74) 29 qui ont défini les principes de la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs privé et public[112]. L'objectif était de favoriser l'élaboration d'une législation nationale inspirée de ces résolutions. Il est alors apparu qu'une protection générale des données à caractère personnel ne serait efficace que si l'on renforçait encore les règles nationales au moyen de normes internationales à caractère contraignant. La même suggestion a été faite lors de la Conférence Européenne des Ministres de la Justice en 1972[113].

Ainsi, la Convention STE N°108 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel voit le jour en 1981. Selon cette Convention, les Parties prennent, dans leur droit interne, les mesures nécessaires pour donner effet aux principes qu'elle pose, à l'égard des données à caractère personnel de tous les individus présents sur leur territoire[114].

Par la suite, on trouve surtout la récente directive 95/46/CE du 24 octobre 1995 relative à *« la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données »*[115].

En vertu de cette directive, toute information, quelque soit son contenu, est considérée comme étant « à caractère personnel » dès l'instant où elle peut être rattachée à un individu déterminé.

Le critère pour l'application d'une loi nationale ayant transposé la directive est en principe le lieu d'établissement du responsable du traitement de données.

Les principes à la base de protection offerte par la directive sont la transparence et la finalité.

Cette directive a été complétée par une autre, la directive 97/66/CE du parlement européen et du Conseil du 15 décembre 1997. Celle-ci concerne le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[116].

---

[112] Disponible sur le site Internet du Conseil de l'Europe, www.coe int.
[113] Voy. le site Internet du Conseil de l'Europe, www.coe int
[114] Disponible sur le site Internet du Conseil de l'Europe, www.coe int
[115] Disponible sur le site Internet duConseil de l'Europe, www.coe int
[116] Disponible sur le site Internet duConseil de l'Europe, www.coe int

C. AU NIVEAU NATIONAL

Dans notre pays, le respect des données à caractère personnel est également ardemment défendu. On trouve ainsi, et principalement[117] :

· La loi du 8 août 1983 organisant le Registre national des personnes physiques

Créé en 1968, le Registre national a été doté d'un cadre légal en 1983[118]. Cette loi introduit un certain nombre de garanties spécifiques concernant la protection de la vie privée, comme par exemple en ce qui concerne les conditions d'accès et de rectification des informations du Registre national.

· La loi du 15 janvier 1990 relative à la Banque-Carrefour de la sécurité sociale

La Banque-Carrefour de la sécurité sociale est organisée par la loi du 15 janvier 1990 modifiée par la loi du 6 août 1990[119].

La Banque-Carrefour, qui est un organisme public doté de la personnalité civile[120], fait office d'organisme carrefour par l'intermédiaire duquel doit se dérouler tout échange de données entre les organismes de sécurité sociale ou entre ces organismes et des tiers.

· La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

Elle vise la protection des secteurs public et privé, les traitements automatisés et manuels et exclut les personnes morales[121]. Cette loi donne également naissance à la Commission de protection de la vie privée.

· La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24/10/95

Modifiant la loi du 8 décembre 1992, elle transpose en droit belge[122] la directive européenne du 24 octobre 1995 relative à *« la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données »*[123].

---

[117] P., GLINEUR, *Droit et éthique de l'informatique*, Bruxelles, Story scientia, A la rencontre du droit, 1991, pp. 54 et s.
[118] L. du 8 août 1983 organisant le Registre national des personnes physiques, *M.B.*, 21 avril 1984, p. 5247.
[119] L. du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.*, 22 février 1990, p. 3288.
[120] P., GLINEUR, *Droit et éthique de l'informatique*, Bruxelles, Story scientia, A la rencontre du droit, 1991, p. 56
[121] L. du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.* 18 mars 1993, p. 5801.

• La Commission de Protection de la Vie Privée

La directive européenne du 24 octobre 1995 prévoit l'existence dans les Etats Membres d'une autorité de contrôle chargée de surveiller sur son territoire l'application des dispositions adoptées en application de la directive. Ce rôle est joué en Belgique par la Commission de Protection de la Vie Privée, instaurée par la loi du 8 décembre 1992[124]. Elle comporte 16 membres : le Président, membre à temps, et d'autres membres choisis pour leur connaissances professionnelles et leur expérience des secteurs publics et privés. On y trouve des magistrats, des professeurs d'université, des juristes, des informaticiens, …

La Commission a plusieurs rôles :

- Elle émet soit d'initiative, soit sur demande du Gouvernement, des Chambres législatives, des Exécutifs communautaires ou régionaux, des Conseils de communauté ou régionaux,… des avis sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée. Ce fut notamment le cas pour la loi du 28 novembre relative à la criminalité informatique ;

- Elle peut également émettre des recommandations sur toute question relative à l'application des principes fondamentaux de la protection la vie privée ;

- Elle examine les plaintes qui lui sont adressées ; les membres de la Commission disposent alors des mêmes pouvoirs d'investigation que les agents de la police judiciaire. Dans le traitement de ces plaintes, la Commission privilégie la recherche de solutions de conciliation entre parties. En l'absence de conciliation, la Commission peut émettre un avis sur le caractère fondé de la plainte, avis qui peut être accompagné de recommandations à l'intention du maître de fichier. Sauf si la loi en dispose autrement, la Commission peut dénoncer au Procureur du Roi les infractions dont elle a connaissance.

- Enfin, la Commission exerce une autorité de tutelle sur les comités de surveillance et de contrôle spécialisés dans des matières bien définies, telles que les banques de données sociales et les banques de données du secteur du crédit.

Cette matière s'éloignant de notre sujet d'étude principal, nous nous permettons de renvoyer aux références bibliographiques indiquées plus tôt.

---

[122] L. du 11 décembre 1998 transposant la directive 95/46/CE du 24/10/95 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.* 3 février 1999, p. 3049.

[123] Cf. Supra.

[124] L. du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.* 18 mars 1993, p. 5801.

Section 3 – Le réseau « Echelon » : la démocratie selon les Etats-Unis

Le réseau Echelon constitue un excellent exemple des problèmes liés au respect de la vie privée dans le réseau Internet (et dans l'ensemble des nouvelles technologies et nouveaux moyens de communications[125]).

Comme nous allons le voir, le réseau Echelon était destiné à surveiller, à espionner les communications (étrangères ou non aux USA) de nature militaire ou relatives à la sécurité du pays.

Or, il apparaît, suite à l'enquête réalisée par le journaliste Duncan Campbell, que le réseau Echelon ne se limiterait pas à ce type d'informations, mais serait plutôt utilisé à des fins privées et économiques.

L'un des points préoccupants qui sera abordé est le fait que si le grand public n'a pas nécessairement connaissance de ce réseau, les états, les gouvernements, en ce compris la Belgique, sont au courant de son existence et de ses capacités, et partant, que celle(s)-ci est (sont) en contradiction avec le respect de différents textes, tant nationaux qu'internationaux.

Mais avant d'entrer plus avant dans les caractéristiques du réseau Echelon, un bref rappel des faits menant à la concrétisation de celui-ci nous parait justifié[126].

A. LE PACTE UKUSA

Lors de la deuxième guerre mondiale, les différentes nations prirent conscience de l'importance de plus en plus croissante de l'information, et partant, des services de renseignements.

Bien qu'ils se soient déjà rencontrés auparavant, les services de renseignements américains et anglais virent leur coopération se renforcer avec l'engagement commun des flottes dans l'Atlantique nord, lors de l'été 1941.

En juin de la même année, les Britanniques réussirent à casser le ENIGMA, le code utilisé par la marine allemande et en 1942, des cryptologues américains de la « Naval SIGINT Agency » commencèrent à travailler aux Royaume-Uni. Les bases d'une alliance SIGINT[127] étaient posées.

En 1943 intervint l'accord BRUSA-SIGINT. Le contenu de celui-ci était le suivant : l'échange de toute information provenant de la découverte, de l'identification et l'écoute de signaux, ainsi que des

---

[125] Nous visons ici les e-mails, les sms, les connexions par satellites, les communications par fax,…

[126] Pour la réalisation de cette partie consacrée au réseau Echelon, nous nous sommes basés principalement sur les sites Intelligence Stratégique , www.intelligence-strategique.fr.st, et Echelon On Line, www.echelon-online.fr.st, Régulièrement mis à jour, ils constituent des véritables base de données sur le réseau.

[127] On entend par « Signal intelligence » des informations à caractère technique et ayant trait aux services d'informations qui sont obtenues par des signaux notamment des télécommunications sans que le destinataire de l'information ne soit impliqué.

algorithmes des codes et clés cryptage. Les Américains étaient compétents pour le Japon, les Anglais pour l'Allemagne et l'Italie.

En septembre 1945, le président Truman signa un mémorandum top secret constituant la clé de voûte d'une alliance SIGINT en temps de paix. Divers accords furent alors pris, fruits d'âpres négociations avec d'autres pays, pour aboutir deux ans plus tard à la conclusion, secrète, d'un pacte de sécurité baptisé « UKUSA ».

L'alliance UKUSA était basée sur les structures anglaises et américaines, issues de leur alliance lors de la deuxième guerre mondiale, ainsi que sur les réseaux de trois pays du Commonwealth, à savoir le Canada, l'Australie et la Nouvelle Zélande.

Plus tard, d'autres pays signèrent les accords SIGINT secrets avec les Etats-Unis : la Norvège, le Danemark, l'Allemagne et la Turquie devinrent ainsi des participants « tiers » dans le réseau UKUSA.

L'objectif principal de ce pacte était la collecte d'informations en provenance de l'URSS et de ses alliés par le biais d'un système d'écoute et d'analyse : le réseau « Echelon ».

A la fin de la guerre froide, les Américains réorienteront leur système de surveillance, pour s'intéresser à leurs concurrents économiques que sont le Japon et les puissances européennes.

La question que l'on peut évidemment se poser est de savoir comment est-il possible d'avoir autant d'informations, de dates, d'éléments sur une alliance secrète, basée sur des accords secrets et visant à obtenir des informations secrètes.

La raison tient en trois lettres : NSA. L'agence de sécurité américaine centralise en effet toutes les données obtenues par le réseau Echelon. C'est elle qui les regroupe, coordonne, redistribue… et donc qui les filtre.

A cela, il faut ajouter les tensions entre partenaires, inhérentes à ce type d'alliance, ainsi qu'une inégalité des forces en présence (seule l'Angleterre dispose des moyens permettant d'analyser les documents et d'instaurer avec les Etats-Unis des relations « moins inégales » qu'avec les autres membres du pacte).

Ainsi, dès 1995, le Canada affirma collaborer avec *« certains de ses plus proches et plus anciens alliés pour l'échange de renseignements extérieurs »*[128].

Tous ces éléments conjugués, ajoutés au changement de gouvernement en Australie et en Nouvelle-Zélande ont abouti à un changement d'attitude de ces deux pays à l'égard du pacte UKUSA, l'Australie affirmant même publiquement que le DSD[129] *« coopère effectivement avec des organisations équivalentes d'espionnage des signaux outre-mer sous l'égide de l'alliance UKUSA »*[130].

---

[128] Echelon On Line, www.echelon-online.fr.st.
[129] Le Defence Signals Directorate est l'agence SIGINT australienne.
[130] Echelon On Line, www.echelon-online.fr.st.

B. LES CARACTÉRISTIQUES DU RÉSEAU ECHELON

1) Echelon : un cran au-dessus des autres

Le réseau Echelon se distingue des autres systèmes de renseignements par le fait qu'il présente trois caractéristiques lui conférant un niveau de qualité tout particulier[131].

Tout d'abord, il est réputé pouvoir exercer une surveillance quasi-totale. Par l'intermédiaire de stations de réception satellitaire et de satellites-espions disséminés à travers le monde sur le territoire des pays alliés, il est capable d'intercepter n'importe quelle information, quel que soit son support (téléphone, Internet, fax,…).

Pour Duncan Campbell, journaliste écossais expert dans l'étude des systèmes de renseignements et en particulier d'Echelon, même si ce type de prouesse technique a souvent été défendu par la presse, ce système a aussi ses limites, comme nous le verrons un peu plus tard.

Ensuite, comme nous l'avons vu, Echelon exerce ses activités au niveau planétaire, grâce à la coopération de plusieurs états (d'où son appellation de « réseau » Echelon), ce qui constitue un atout indéniable par rapport aux systèmes nationaux.

Cette coopération internationale est essentielle pour la surveillance à l'échelle mondiale, car elle seule permet d'intercepter les deux liaisons de données air/sol, et donc, les deux parties d'une conversation.

Mais, plus qu'un atout, cette coopération est avant tout une nécessité. En effet, compte tenu de leurs dimensions, les stations de réception satellitaire ne peuvent être construites sur le territoire d'un pays sans son assentiment.

PAYS	AGENCES	PRINCIPAUX TERRITOIRES COUVERTS
ROYAUME-UNI	*The United Kingdom's Government Communication Headquarter (GCHQ)*	L'Afrique, l'Europe contientale et la Russie européenne
AUSTRALIE	*Australia's Defense Signals Directorate (DSD)*	L'Asie du Sud-Est et la Chine méridionale
NOUVELLE-ZÉLANDE	*New Zealand's Government Communication Security Bureau (GCSB)*	La zone du Pacifique
CANADA	*Centre de la sécurité des télécommunications (CST)*	Le nord de la Russie et probablement l'Amérique latine
ÉTATS-UNIS	*National Security Agency (NSA)*	L'Amérique du Sud, l'Asie, la Russie asiatique et la Chine

Ce tableau reprend les différents pays et agences de renseignements nationales et les territoires couverts par leur surveillance[132].

Enfin, comme nous l'avons déjà souligné, Echelon serait réputé, depuis plusieurs années, avoir délaissé ses objectifs de type militaire pour se concentrer sur des objectifs économiques ou privés.

Dans son rapport commandé par le STOA[133], Duncan Campbell étaie cette thèse par divers exemples, comme l'affaire Airbus[134].

En 1994, dans le cadre d'un contrat d'achat d'avions de 6 milliards de $ entre Airbus et une compagnie d'Arabie Saoudite, la NSA a intercepté les fax et communications téléphoniques que ceux-ci s'échangeaient. Les informations ainsi collectées ont été transmises à Boeig et Mc Donell-Douglas, permettant ainsi à ce dernier d'obtenir le marché[135].

Au passage, une manœuvre de corruption d'Airbus (à savoir des pots de vin offerts à des membres de la commission chargée d'attribuer le marché) a été mise à jour, empêchant ainsi les Européens de dénoncer ce procédé et/ou justifiant l'action des Américains au regard du comportement déloyal des européens (nous verrons plus tard que c'est en grande partie l'explication avancée par les Etats-Unis pour justifier ces pratiques).

2) Echelon : qualité filtre

Le réseau Echelon filtre près de deux millions de e-mails par heure, pour finalement n'en retenir que quatre, cette activité mobilisant 90000 personnes et 20 milliards de dollars par an.

Il utilise un système de croisement de mots-clés qui permettent aux automates de traitement de sélectionner les e-mails intéressants qui seront étudiés en détail[136].

Mais, si Echelon utilise près de 10000 mots-clés, beaucoup de messages passent à travers les mailles du filet.

Des internautes avaient d'ailleurs pensé avoir trouvé la parade : ils remplissaient leurs e-mails de mots-clés, tels que « terrorism », « bomb », « explosion », « chimical »,… afin de saturer les automates. Seulement, Echelon est très bien conçu et si trop de mots-clés polluent un message, Echelon ne le traite pas.

Evidemment, ce type de démarche n'est pas infaillible, dans un cas comme dans l'autre : les e-mails peuvent contenir « trop peu » de mots-clés que pour ne pas être retenus par Echelon et celui-ci peut ne pas traiter un message intéressant mais noyé parmi des dizaines de mots-clés.

---

[131] S., WRIGHT, *Une évaluation des techniques de contrôle politique, étude intérimaire STOA*, PE 166.499,1998, pp. 20 et ss.
[132] Ces informations proviennent du site Echelon On Line, www.echelon-online.fr.st.
[133] STOA (Evaluation des choix scientifiques et techniques) est le service de la Direction générale des études du Parlement européen qui confie des travaux de recherche à l'extérieur, à la demande des commissions.
[134] Il y a plusieurs affaires dans lesquelles Echelon est ou serait impliqué, comme lors des négociations du GATT (en 1993), l'affaire Thomson-CSF (en 1994), l'affaire Enercon (en 1996),…
[135] Echelon On Line, www.echelon-online.fr.st.
[136] Intelligence stratégique, www.intelligence-strategique.fr.st.

Un autre moyen permettant de passer au travers du filet tendu par le réseau Echelon consiste en le cryptage des messages.

Le plus connu des logiciels de cryptage est certainement PGP, pour « Pretty Good Privacy » (« une défense plutôt bonne »)[137]. Ce nom a été choisi à bon escient car il illustre bien le fait que le système de défense absolue contre la surveillance électronique n'existe pas.

Pour ne pas entrer dans des détails trop techniques, disons que la différence entre envoyer un e-mail normal et un e-mail codé avec PGP est la même qu'envoyer une carte postale et envoyer une carte postale dans une enveloppe.

Dans la cas de l'enveloppe, il faut l'ouvrir et donc savoir auparavant qu'il y a quelque chose d'intéressant dans celle-ci. La même logique s'applique aux e-mails codés. Si Echelon décide de décrypter un message, il lui faudra entre 1 et 2 semaines pour le faire. Dès lors, Echelon se retrouve devant un problème sans solution : comment décider si un message crypté est important ou non, sans connaître, par avance, le contenu de celui-ci ? PGP ne permet en réalité qu'une seule chose : cacher aux yeux de tous si le contenu est intéressant ou non, le cryptage/décryptage n'étant finalement que secondaire (face à Echelon du moins).

Par contre, il est évident que Echelon montre un réel intérêt lorsqu'il s'agira de filtrer, de décrypter et d'analyser les messages d'une personne déterminée.

Mais dans les autres cas, la probabilité que Echelon intercepte et décrypte (ou décide de crypter) un message parmi des dizaines de millions d'autres est très faible.

[137] Ce logiciel est disponible à l'adresse www.pgp.com.

C. LA COMPATIBILITÉ AVEC LE DROIT FONDAMENTAL AU RESPECT DE LA VIE PRIVÉE

L'article 8 de la Convention européenne des droits de l'Homme (CEDH), qui consacre le droit à la vie privée, autorise les atteintes à celle-ci pour préserver la sécurité nationale dans certains cas : il faut que les dispositions du droit national prévoient cette atteinte et que ces dispositions soient accessibles à tous, et qu'elles définissent les circonstances et conditions dans lesquelles les pouvoirs publics pourront y recourir[138]. Ces atteintes devront être proportionnées, ce qui implique que les intérêts des différentes parties soient mis en balance, de sorte qu'il ne suffise pas qu'elles soient simplement opportunes et/ou souhaitables.

Dès lors, un système de renseignement qui intercepterait, sans distinction et en permanence, des communications violerait le principe de proportionnalité et serait donc contraire à la CEDH. De même, la CEDH serait également violée si les dispositions en vertu desquelles la surveillance est opérée se trouvaient être sans fondement juridique, et/ou si celui-ci n'était pas accessible à tous.

A ce stade de notre exposé, il nous paraît pertinent de préciser la position des Etats-Unis sur le réseau Echelon et plus particulièrement sur sa raison d'être. Cette position est clairement (et longuement) expliquée par James Woosley, l'ancien directeur de la CIA de 1993 à 1995[139]. En voici quelques extraits choisis :

« (…) Oui, chers amis du continent européen, des mots clés. Vous êtes-vous posé la question de savoir ce que nous cherchons ?

Le récent rapport au Parlement européen sur Echelon, écrit par le journaliste britannique Duncan Campbell, a déclenché de furieuses accusations. En provenance de l'Europe continentale. Selon lesquelles les services de renseignement américains volent les technologies avancées des compagnies européennes pour que nous puissions – notez-le – les donner aux compagnies américaines pour les aider à rester compétitives. Mes amis européens, redescendez sur terre. C'est vrai, dans une poignée de domaines, la technologie européenne surpasse l'américaine, mais, pour le dire aussi aimablement que possible, ces domaines sont en très, très, très petit nombre. La plupart des technologies européennes ne méritent pas que nous les volions.

Pourquoi, donc, vous avons-nous espionnés ? La réponse se trouve dans le rapport Campbell, dans l'analyse des deux seuls cas où il est dit que des compagnies européennes auraient été les cibles de la collecte américaine de renseignements. A propos de Thomson-CSF, le rapport indique : la compagnie était largement suspectée d'avoir corrompu des membres du

---

[138] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et Protocole additionnel, signé à Paris le 20 mars 1952, approuvés par la loi du 13 mai 1955, *M.B.*,19 août 1955.
[139] J., WOOSLEY, « Why America Spies on its Allies », Washington Post, 17 mars 2000.

comité de sélection du gouvernement brésilien. D'Airbus, il dit que nous avons pu prouver que ses agents offraient des pots-de-vin à un officiel saoudien. Ces faits sont systématiquement omis dans les articles de presse européens.

Eh oui, chers amis continentaux. Nous vous avons espionnés parce que vous distribuez des pots-de-vin. (...).

Quels sont les secrets économiques, au-delà des tentatives de corruption, que nous avons voulu obtenir par l'espionnage ? Il s'agit par exemple des tentatives de certaines sociétés de masquer le transfert de technologies à usage dual. Nous suivons de près les ventes de super-ordinateurs et de certains produits chimiques, car ils peuvent être utilises non seulement pour des objectifs commerciaux mais aussi pour soumis à des sanctions – l'activité bancaire serbe, le trafic de pétrole irakien. (…)

Européens. Soyez sérieux. Cessez de nous critiquer et réformez vos propres politiques économiques étatiques. (…)

Et nous, nous n'aurons plus besoin de vous espionner ».

Sans susciter d'analyse très pointue, la position américaine nous semble claire : nous vous espionnons parce que vous trichez, arrêtez de tricher et nous arrêterons de vous espionner.

Cette réaction de la part de James Woosley est assez facile ou très naïve.

En effet, il nous paraît difficilement imaginable de dépenser 20 milliards de $ par an et mobiliser près de 100.000 personnes uniquement pour espionner les tentatives de corruption européennes. De deux choses l'une : ou le réseau Echelon est particulièrement peu productif, ou James Woosley possède une mémoire très sélective. Chacun appréciera.

De plus, Woosley occulte les autres affaires dans lesquelles Echelon est ou serait impliqué, comme les négociations du GATT[140] ou l'affaire Enercon[141] par exemple.

Enfin, il est intéressant de constater l'habileté avec laquelle l'ancien directeur de la CIA transforme une atteinte au droit fondamental à la vie privée (et donc une violation à la CEDH et à nombre de dispositions nationales) en un service rendu au monde et à la société économique.

---

[140] Lors des accords du GATT, en 1993, toutes les conversations des participants français ont été espionnés, en particulier celles du ministre des affaires étrangères Alain Juppé.

[141] A. Wobben, Ingénieur de la société allemande Enercon, avait mis au point une éolienne de haute technologie pour la production d'électricité. Ayant pris connaissance de ses travaux, la NSA les transmet à une société américaine qui s'empresse de déposer les brevets relatifs à cette découverte. Enercon obtint justice, mais ses ambitions de pénétration du marché américain furent complètement anéanties.

Pour en revenir à la CEDH, il nous faut pointer que même si les Etats-Unis ne sont pas partie à la convention, les Etats membres se doivent de respecter celle-ci, et donc, ne peuvent autoriser les services de renseignements d'un pays soumis à des dispositions moins rigoureuses à opérer sur leur territoire. Si tel était le cas, le principe de légalité (et ses deux composantes que sont l'accès et la prévisibilité) serait privé de ses effets et la jurisprudence de la Cour européenne de droits de l'Homme serait vidée de sa substance.

La conformité d'une activité d'un service de renseignements aux droits fondamentaux nécessite l'existence de dispositifs de contrôle suffisants afin de parer aux risques inhérents à ce type d'activité.

A ce titre, il faut souligner que, si dans la majorité des Etats membres, le droit à la vie privée est inscrit dans la constitution, certains d'entre eux ne disposent pas d'organes de contrôles parlementaires des services secrets. Ainsi, la Finlande et la Suède confient le contrôle parlementaire des services secrets à des médiateurs indépendants nommés par le parlement, et le Royaume-Uni ne surveille que les services de renseignements civils[142].

Un autre point est également à souligner : un système d'interception des communications internationales comme Echelon ne vise pour la plupart du temps pas les habitants du pays qui l'exploite. Dès lors, de par son statut d'étranger, la personne dont les messages, conversations, courriers sont interceptés, ne dispose d'aucune protection juridique dans le pays «espion ». Le contrôle parlementaire risque de ne pas être suffisant dès lors que les électeurs, partant du principe qu'ils ne sont pas concernés (les seules à être concernées étant des personnes à l'étranger), peuvent ne pas manifester une intérêt particulier pour cette question, et donc que pour les élus, seuls les intérêts des électeurs doivent être pris en compte[143]. Ainsi, à titre d'exemple, les auditions sur les activités de la NSA qui ont lieu au sein du Congrès américain, avaient pour seul but de savoir si des citoyens américains étaient victimes de ce type de surveillance[144].

Enfin, il nous semblait intéressant de donner quelques précisions sur la position de la Belgique vis-à-vis du réseau Echelon[145].

---

[142] G., SCHMID (Rapporteur), *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, Commission temporaire sur le système d'interceptions Echelon*, PE 305.391, 2001, p. 103.

[143] Ceci n'est évidemment pas une généralité, mais montre que le contrôle parlementaire n'est pas la solution miracle à ce problème.

[144] G., SCHMID (Rapporteur), *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, Commission temporaire sur le système d'interceptions Echelon*, PE 305.391, 2001, p. 27

[145] Pour ce qui concerne l'analyse des différents systèmes européens, nous invitons nos lecteurs à consulter, entre autres, les différents rapports et documents de travail publiés par la commission européenne (ils sont notamment accessibles à l'adresse www.europarl.eu.int/committees/echelon_home.htm). Celle-ci a commencé à s'intéresser au problème suscité par Echelon suite à l'étude que le STOA avait commandée à Duncan Campbell. Ce rapport a été présenté à l'occasion d'une audition de la commission des libertés et des droits des citoyens, de la justice et des affaires intérieures ayant pour thème « l'Union européenne et la protection de données ».

D. LA SITUATION EN BELGIQUE

Le comité permanent R du sénat belge[146] a déjà rendu deux rapports sur le réseau Echelon.

Tout d'abord, un chapitre du « Rapport d'activités 1999 » est entièrement consacré aux réactions des services belges de renseignements par rapport à l'existence, avérée ou non, du système Echelon.

Les auteurs parviennent à la conclusion que les seules informations obtenues par les deux services belges de renseignements que sont la Sûreté de l'Etat et le Service Général du Renseignement (SGR) proviennent de documents publics.

Ensuite, le «Rapport complémentaire d'activités 1999 » traite du système Echelon de manière plus approfondie, se prononçant notamment sur les études STOA.

Il ressort de ce rapport que le réseau Echelon existe réellement et permet de capter toutes les informations transmises par satellite.

Les auteurs soulignent également l'impossibilité d'établir ce que fait et ce que ne fait pas Echelon.

Des questions ont également été posées par certains parlementaires. En voici deux qui nous ont semblé intéressantes quant à la position de la Belgique et à ses futurs engagements[147].

Tout d'abord, ce sont les sénateurs Josy Dubié, Frans Lozie et George Dallemagne qui ont adressé, le 17 février 2000, plusieurs questions au vice-premier ministre et ministre des affaires étrangères Louis Michel, relatives notamment à l'existence d'Echelon.

Pour Louis Michel, l'existence du réseau Echelon est on ne peut plus vraisemblable, et si son existence était confirmée, le gouvernement belge serait face à une situation inacceptable.

Louis Michel propose donc d'analyser les incidences d'Echelon sur la société belge afin d'assurer l'intégrité du pays, mais également de tout mettre en œuvre afin d'en mesurer les conséquences économiques et sociales.

Le 6 juillet 2000, c'est au tour de Philippe Moureaux d'interroger le ministre des affaires étrangères, cette fois sur la possibilité de saisir la Cour européenne des droits de l'Homme pour violations des droits garantis par la Convention.

Suppléant le ministre des affaires étrangères, c'est Rick Daems qui répond.

---

[146] Le Comité permanent de contrôle des services de renseignements et de sécurité se compose de trois membres nommés par le Sénat ; au Comité R est adjoint un service des enquêtes dont les membres sont nommés par le Comité R.

[147] G., SCHMID (Rapporteur), *Document de travail*, Commission temporaire sur le système d'interception Echelon, PE 294.297/6REV, 2001, pp. 37 et suiv.

Sur le plan juridique, le peu d'informations sur les fondements politiques et légaux du système Echelon ne permet pas d'établir des responsabilités et la recherche d'une base juridique afin de déposer plainte.

En ce qui concerne le droit à la vie privée consacré à l'article 8 de la CEDH, le ministre fait observer que si certaines ingérences sont admissibles, la préservation d'intérêts économiques ne sont pas une justification valable.

Par ailleurs, la structure (supposée) du réseau, son origine extra-européenne et l'étendue de son rayon d'action ne sont pas de nature à faciliter la saisine de la Cour. L'exécution des jugements de cette Cour étant du ressort de l'Etat concerné, le mécanisme de protection des droits de l'Homme sur le plan européen ne permet guère de faire face à un système transnational créé par plusieurs Etats.

De plus, il paraît peu probable qu'une plainte communautaire recueille l'assentiment de tous les Etats membres de l'Union européenne, et à l'inverse, l'action d'un seul Etat serait difficile à engager étant donné la complexité du dossier.

Le ministre des affaires étrangères estime donc que les inconvénients d'une telle démarche l'emportent, pour la Belgique, sur ses avantages symboliques[148].

La position belge est donc claire. Bien que l'existence d'Echelon soit de plus en plus confirmée, la (petite) Belgique ne sera pas à même de défendre les intérêts de ses citoyens, à moins d'entacher ses relations diplomatiques et économiques.

Pour notre part, nous pensons qu'une partie des réticences vient de la complexité de l'adversaire, qui est à la fois américain en grande partie, mais également anglo-saxon (les autres pays commençant, comme nous l'avons vu, à se désolidariser de l'ancienne alliance UKUSA). L'adversaire est donc à la fois un géant, les Etats-Unis, sur le pan politique, économique, diplomatique d'un côté, et un partenaire de premier ordre, l'Angleterre, au sein-même de l'Union européenne.

Il est certain qu'il sera difficile de voir l'assentiment de l'ensemble des pays de l'Union européenne, et donc parmi eux l'Angleterre, à entamer une lutte contre Echelon.

Et ce d'autant plus, qu'un projet européen similaire à Echelon est en train de voir le jour.

---

[148] G., SCHMID (Rapporteur), *Document de travail*, Commission temporaire sur le système d'interception Echelon, PE 294.297/6REV, 2001, p. 38

E. LA BOUCLE EST BOUCLÉE : L'ECHELON EUROPÉEN

Face à la menace (aux avantages ?) que représente Echelon, un projet européen est actuellement mis en place, projet auquel, bien entendu, les Etats-Unis sont farouchement opposés.

Plusieurs problèmes viennent déjà salir ce bel édifice.

Tout d'abord, l'Angleterre va devoir s'affranchir de ses alliances avec les Etats-Unis, ce qui ne sera pas facile notamment en raison de sa collaboration sur la plan technique et logistique.

Ensuite, voyant l'émergence d'un axe France-Allemagne au niveau de l'intelligence économique, les Etats-Unis tentent de partager Echelon avec le plus de pays européens possibles, tout en tenant l'Allemagne et la France à l'écart. Le Danemark, la Suisse et la Finlande sont ainsi déjà du côté des Etats-Unis. Nous pointons que cette dernière position des Etats-Unis semble logique d'un point de vue économique et diplomatique (stratégique), mais va totalement à l'encontre des bonnes intentions prônées par James Woosley concernant l'utilisation du réseau Echelon[149].

[149] CF. supra.

Section 4 –- Conclusion

Pour les raisons qui ont été évoquées plus tôt, nous nous attarderons, pour cette conclusion, essentiellement sur le réseau Echelon.

Si la vraisemblance de l'existence du réseau Echelon et de ses capacités n'est plus véritablement une question à se poser, ce n'est pas le cas de la réaction à adopter.

Nous constatons ainsi que plutôt que de s'opposer à « l'ennemi », l'Union européenne a choisi d'adopter les mêmes méthodes que lui. La question à se poser sera dès lors de savoir si cette attitude permettra de rétablir la balance, ou au contraire, en raison du caractère secret lié à ce type de démarche, d'augmenter, d'aggraver les violations des droits des citoyens. Ceux-ci ne seront en effet plus seulement espionnés en Europe, mais sur l'ensemble du globe.

A notre sens, il est clair que le fait-même de choisir de mettre en place un Echelon européen entraîne ipso facto l'impossibilité de revenir en arrière et donc d'empêcher que le réseau Echelon existant de continuer ses agissements. C'était certes la solution la plus difficile, la plus risquée, mais c'était pourtant surtout la plus sensée.

Dorénavant, la solution adoptée est similaire à celle apportée au problème de l'armement nucléaire : au désarmement, plus difficile, plus utopique peut-être, a été préféré l'escalade « nucléaire », chaque pays étant tenu en joue tout en pointant son arme sur son adversaire potentiel.

Désormais, nous espionnerons notre voisin tout en sachant qu'il nous espionne.

Belle perspective…

Enfin, il nous faut aborder ce qui est peut-être le point le plus important de cette partie consacrée au réseau Echelon.

Il nous semble en effet paradoxal de voir des lois commencer à abonder sur la problématique du hacking, alors que rien, ou presque ne s'applique à Echelon.

Si le piratage opéré par un « particulier » est un crime, il apparaît que le piratage opéré par un Etat serait soit un service rendu au marché économique (comme nous l'expliquait James Woosley), soit une nécessité afin de maintenir un certain équilibre entre espions et espionnés.

Le but ici n'est certainement pas de dire que le piratage opéré par les hackers n'est pas grave par rapport aux violations opérées à l'échelle étatique, mais bien de montrer qu'il existe une différence entre établir, consacrer une norme et (pouvoir) l'appliquer.

De même, sans nécessairement se placer sur le plan juridique, comment expliquer que des crimes soient punis ou acceptés (de bon ou mal gré) en raison de la qualité de l'infracteur ?

Imagine-t-on de ne pas poursuivre un voleur parce qu'il est un industriel important ? D'autoriser les autorités à utiliser n'importe quelle méthode en vue de lutter contre des infractions ?

La réponse est évidemment non[150], mais il semble, à la lecture de l'analyse qui précède, que c'est pourtant bien de ce type de « privilège » dont le réseau Echelon, et ceux qui l'exploitent, bénéficient.

Il est important d'avoir à l'esprit que ce n'est pas l'action de l'Etat qui est la source de sa légitimité, mais bien le contraire. Certains actes sont autorisés ou non en fonction de lois, normes, et non en fonction d'une position stratégique sur l'échiquier politique mondial.

Il est évident que les propos tenus ici ne sont que théoriques, et que toutes les subtilités de la diplomatie internationale nous échappent certainement, mais il nous semble que l'aspect de résignation, l'absence de contestation suivie d'effets de la part des états concernés (espionnés) est préoccupante.

Le fait de ne pouvoir empêcher une infraction de se commettre ne devrait pas être un obstacle à sa contestation.

[150] Nous visons ici la situation idéale, celle qui devrait exister, et donc pas nécessairement celle existant « réellement », actuellement.

Deuxième Partie – Le monde des hackers

Après avoir posé les principaux éléments de la criminalité informatique, il est temps à présent de nous intéresser plus spécifiquement aux auteurs de ces crimes informatiques, à savoir aux hackers.

Cette partie aura pour but, entre autres, de démontrer que la représentation classique du hackers réalisés par les médias est loin de la réalité du monde de pirates informatiques.

Pour étayer notre propos, nous allons d'abord nous intéresser à l'historique du hacking. Nous présenterons l'histoire des premiers hackers, débutant dans les années 1960 s'étalant sur plus de trente ans.

Ensuite, nous attarderons longuement sur les caractéristiques des hackers. Nous verrons, entre autres, quelles sont les différentes catégories de hackers, quelles sont leurs motivations ou encore leur vision du Bien et du Mal. Ces caractéristiques permettront de comprendre, notamment au regard de leurs motivations, quels doivent être les moyens mis en œuvre afin de lutter contre la criminalité informatique.

Cette partie sera également l'occasion de souligner la pertinence de certaines théories criminologiques appliquées au monde des hackers, comme celles développées par Sutherland, Merton ou encore Sellin.

Pour terminer, nous aborderons rapidement l'arsenal des hackers, en soulignant d'ores et déjà que le point important de cette partie sera l'analyse de l'ingénierie sociale, en raison du rôle joué par celle-ci dans l'efficacité des mesures de prévention.

Titre I – Historique du hacking

Cet historique a pour but principal d'expliquer comment les hackers, au départ bidouilleurs passionnés, généralement respectueux des lois, sont devenus les cybercriminels qui défrayent aujourd'hui la chronique des journaux.

Après avoir expliqué les principales innovations technologiques amenant les hackers à se structurer, nous verrons comment leur alliance avec les phreakers va être déterminantes pour leurs mouvements respectifs.

Ensuite viendra l'explication du glissement des hackers vers le cybercrime et le conflit des générations en ayant découlé.

Nous terminerons par une rapide présentations des hackers les plus célèbres et les plus importants pour l'histoire du mouvement.

Section 1 – De l'Altair au Captain Crunch

Notre historique débute aux Etats-Unis, au début des années 70[151]. Dans un garage, une trentaine de jeunes californiens s'affairent autour de la drôle de boîte apportée par l'un d'eux. Ce boîtier noir, sans clavier ni écran est actionné par une rangée d'interrupteurs alignés sur sa façade et les résultats se lisent sur les diodes. Il s'agit de l'Altair 8800, l'un des premiers micro-ordinateurs[152].

L'ensemble de ces jeunes mordus de technologie forme le noyau du HomeBrew Computer Club (le club de l'informatique «brassé à la maison»), qui deviendra la matrice de la révolution future de l'ordinateur pour tous[153].

Si l'Altair nous semble rudimentaire, il marque une nette avancée, notamment lorsqu'on le compare à l'un des premiers ordinateurs, l'Eniac, datant de 1946 et pesant 30 tonnes ![154]

Avec l'invention du transistor, les ordinateurs vont subir une cure d'amincissement et coloniser les entreprises pour la comptabilité, les services de recensement du gouvernement,…

Les micro-ordinateurs franchiront une étape supplémentaire : on peut les emmener à la maison.

---

[151] Cette partie est principalement le fruit de l'analyse de deux ouvrages : F., LATRIVE, DUFRESNE, D., *Pirates et flics du Net*, Paris, Seuil, 2000, et BANCAl, D., *Hackers et pirates sur Internet*, Desmaret, 2001.

[152] Le premier micro-ordinateur est le Micral, inventé par Français Gernelle et André Truong deux ans avant l'Altair. La diffusion du Micral restera confidentielle, contrairement à l'Altair.

[153] Il nous faut pointer le fait que la majorité des hackers, à cette époque, se trouve aux Etats-Unis. L'explication est simple : ils commencèrent leurs expérimentations sur l'Altair, mais celui-ci n'était pas commercialisé en Europe, ou de manière très confidentielle.

[154] F., LATRIVE, DUFRESNE, D., *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 13 et suiv.

Calqué sur le modèle du HomeBrew Computer Club, des dizaines de clubs apparaissent sur le territoire américain. Lors de ces réunions se rencontrent des étudiants, des jeunes ingénieurs, des électroniciens confrontant leurs connaissances et leur goût pour le bidouillage. Car il faut préciser que leurs machines n'avaient rien de commun avec nos ordinateurs actuels et avec leur (relative) facilité d'utilisation. Les programmes devaient être disséqués, hachés (*to hack*[155], en anglais), triturer afin de les faire fonctionner.

Au milieu des années 70, le «hacker » n'est pas encore le pirate qu'il est devenu aujourd'hui[156], mais bien un programmeur de talent.

Il nous faut apporter une précision importante sur ce dernier point. Ces jeunes adeptes de la micro-informatique n'étaient pas encore des «hackers ». Ce titre n'est attribué qu'a posteriori, une fois le « hack »[157] validé par l'histoire.

De même, si le terme «hacker » désigne aujourd'hui des criminels ingénieux, les idoles de ces jeunes étaient avant tout des programmeurs devenus célèbres en raison de leurs découvertes ou de leurs créations. Ils admirent ainsi Richard Stallman, as du clavier du célèbre Massachusstts Institute of Technology (MIT), ou encore Ken Thompson et Dennis Ritchie, les concepteurs du système Unix.

Nous ne tenons pas à avoir ici une approche naïve de l'histoire du piratage informatique, mais bien pointer que la démarche de ces jeunes, leur manière d'envisager le hacking est très différente de celle des hackers des années 90[158]. Ainsi, si l'on prend l'exemple de Thompson et Ritchie, leur but premier était de créer un système d'exploitation utile à tous. De même, lorsque Don Bricklin et Bob Frankston font la démonstration en 1978 d'une « feuille de calcul », ancêtre du célèbre Excel de Microsoft, leur but est de travailler, de faire avancer la collectivité.

Bien sûr, la recherche de profit était peut-être présente, mais uniquement sur base des règles commerciales, et non consécutive d'une activité criminelle.

Pour résumer cette période, nous pourrions dire que le but de chaque hacker était d'épater pour faire progresser.

Toujours avides de connaissances, les hackers se trouvaient devant un obstacle de poids : la nécessité de communiquer. En effet, s'il leur était facile de se rencontrer et d'organiser des réunions entre eux, il leur était par contre beaucoup plus difficile d'échanger des informations avec d'autres hackers situés aux quatre coins des Etats-Unis.

---

[155] C'est bien sûr de là que vient le terme « hacker ».
[156] Il est très rare, actuellement, de voir le terme « hacker » désigner autre chose qu'un délinquant informatique.
[157] Il s'agit d'un terme désignant un acte de piratage informatique, d'intrusion.
[158] Nous reviendrons plus tard sur la distinction entre ces différentes générations de hackers.

L'échange d'informations était possible, mais seulement, soit via le téléphone – ce qui revenait très cher, surtout pour une majorité de hackers qui étaient encore pour la plupart étudiants -, soit via l'ancêtre du réseau Internet, Arpanet, créé en 1969, auquel peu de personnes avaient alors accès.

Ce problème de taille nécessitait une solution, et si possible ingénieuse, comme tout hack qui se respecte. C'est John Draper qui va la trouver, devenant ainsi le premier « *phreaker* »[159] de l'histoire.

En 1965, Draper découvre qu'un sifflet offert dans les boîtes de céréales « Cap'n Crunch » émet une tonalité de 2600 mégahertz. Le hasard veut que ce soit également la fréquence audio utilisée par les réparateurs de téléphone pour accéder à une ligne de téléphone depuis l'extérieur. Sans entrer dans des détails techniques, disons que le sifflement déclenchait un signal qui commandait au central téléphonique de ne pas facturer l'appel.

Mieux, cette fréquence correspondait au code d'accès d'AT&T, le plus important opérateur téléphonique américain, utilisé pour les appels interurbains. Draper, baptisé désormais « Captain Crunch », venait de trouver le moyen de téléphoner gratuitement.

Mais, outre ce gain conséquent sur le plan financier, le but premier était surtout de comprendre comment fonctionnaient les réseaux téléphoniques, Draper ayant même, selon la légende, effectué un appel interurbain à partir d'une cabine téléphonique et fait répercuter celui-ci à travers le monde pour le faire finalement aboutir dans la cabine voisine !

[159] Le phreaking sera abordé plus tard.

Section 2 – Hackers et phreakers : l'union sacrée

Cette partie de notre exposé commence en février 1878, à New Haven, aux Etats-Unis, dans les locaux de la compagnie de téléphone Bell.

La compagnie de téléphone avait engagé depuis quelques semaines déjà, un groupe d'étudiants, afin de mettre les utilisateurs des lignes téléphoniques en relation les uns avec les autres, en branchant les lignes téléphoniques sur l'énorme panneau prévu à cet effet.

Si les choses paraissaient simples, il apparaissait que beaucoup d'abonnés se plaignaient de bruits sur la ligne, quand ils n'étaient pas tout simplement connectés au mauvais correspondant.

L'enquête alors entamée révélera que les jeunes garçons, afin de rompre la monotonie de leur travail, avaient commencé à écouter les conversations, allant parfois jusqu'à participer aux conversations.

La société Bell congédia l'ensemble des employés et n'engagea, par la suite, exclusivement que des jeunes femmes, réputées, à tort ou à raison, plus sérieuses dans leur travail, au point que celles-ci deviendront la figure emblématique de la société téléphonique.

Ces jeunes gens, poussés par l'envie de faire une bonne farce plutôt que de véritablement nuire, étaient les premiers «*pranksters* » (« farceurs ») des «nouvelles technologies » d'alors, utilisant les failles d'un système embryonnaire afin de commettre leurs méfaits[160].

Un siècle plus tard, les pranksters laisseront la place aux phreakers, qui se spécialiseront également dans la fraude aux opérateurs de télécommunications.

Le phreaking, qui est un néologisme construit sur base des mots « *freak* » (« mordu/bizarre »),« *free* » (« gratuit »), «*phone* » (« téléphone ») et «hacker », est un mouvement technologique, anti-institutions, anarchiste et parfois New Age, mâtiné de musique et parfois de drogue.

Les phreakers, comme les pranksters, ont pour but de ne pas payer les communications téléphoniques et de pirater les lignes téléphoniques[161].

Comme nous l'avons dit, John Draper est le premier phreaker. Bien qu'il soit devenu un hacker réputé depuis qu'il a découvert comment téléphoner gratuitement, il décide de s'attaquer à un plus gros morceau, et va pour cela demander l'aide de deux amis, Steve Jobs et Steve Wozniak[162].

Ensemble, ils vont créer la « blue-box »[163], qui va être à l'origine du développement de la communauté des phreakers. En effet, ce petit boîtier permet, en envoyant des impulsions selon un certain ordre et une certaine durée précise, de bloquer la facturation des communications sans éveiller

---

[160] J.-S., COUTU, « Pirates du cyberespace », Quebec Micro (http://www.quebecmicro.com), janvier 1999.
[161] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 14 et suiv.
[162] Comme nous le verrons, Jobs et Wozniak créeront plus tard la société Apple et le Macintosh.
[163] D., LABROSSE, « Hackers, la cyberculture à ses extrêmes », http://www.er.uqam.ca (Université du Québec à Montréal), 2001.

les soupçons des opérateurs. Et la suprématie de la petite boîte bleue va durer près de dix ans, pendant lesquels les grandes centrales téléphoniques seront incapables de parer ces actes de piratage.

Forts de leurs succès, les phreakers vont même jusqu'à organiser des « *Party lines* » à l'occasion desquelles plusieurs dizaines de phreakers se réunissent et discutent, sans payer le moindre cent.
Cette période d'euphorie et de relative confidentialité vis-à-vis du grand public prendra fin en 1971. En octobre de cette année, paraît, dans le magazine Esquire, l'article de Rosenbaum « *Secrets of the Little Bue Box* », dévoilant au public américain l'existence des phreakers et de leurs activités.

Cet article est un fait marquant dans l'histoire du phreaking car sa publication conduira plusieurs états américains à prendre des mesures sur le plan légal afin de lutter contre ce type de pratique[164].

La création et l'utilisation de la blue box est déterminante pour l'explosion de la Scène[165]. C'est en effet elle qui va véritablement forger l'alliance entre hackers et phreakers, alliance qui était inévitable afin d'assurer la pérennité et la longévité des deux groupes : les hackers avaient besoin des phreakers pour leur permettre de communiquer à moindre frais et les phreakers avaient besoin des connaissances techniques des hackers afin d'approfondir leurs propres connaissances des centraux téléphoniques et de systèmes de fraudes envisageables.

Cette rencontre entre hackers et phreakers sera scellée par la naissance du mouvement « 2600 », qui deviendra par la suite une organisation reconnue, avec un site officiel (www.2600.org), publiant même un magazine trimestriel tout à fait officiel[166].

Cette alliance est toujours une réalité aujourd'hui. Pour preuve, parmi d'autres, le fait que la blue box est toujours utilisée par des milliers de pirates de par le monde. Celle-ci a dû être modifiée au cours des années afin de contourner les nouvelles protections mises en place par les sociétés téléphoniques, et ces modifications sont le fruit du travail combiné des hackers et des phreakers. Plus qu'alliés, ils sont indissociables les uns des autres, la disparition d'un groupe entraînant à plus ou moins court terme la disparition de l'autre groupe.

Et c'est également cette union inévitable qui va conduire certains hackers à dépasser les frontières de la légalité et à glisser vers le crime informatique, les phreakers étant, de par la nature de leurs actes, déjà dans l'illégalité.

---

[164] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 14 et suiv.
[165] La « Scène » (hacker), représente une sorte d'ensemble, non déterminé, où l'on retrouve pêle-mêle apprentis pirates, corsaires libertataires et hackers confirmés et reconnus.
[166] Y., EUDES, « www.2600.org », Le Monde, 26 janvier 2001.

Section 3 – Le glissement vers le cybercrime

C'est surtout dans les universités que les apprentis délinquants vont se développer. Forts de leurs nouvelles connaissances, certains étudiants vont alors commencer à expérimenter tous azimuts, flirtant souvent avec les limites de la légalité, certains les dépassant.

C'est ainsi que Robert Morris, fils d'un grand dirigeant de la NSA, va créer en 1988 un virus informatique, par curiosité.

Capable de se dupliquer de machines en machines, le virus va être lâché sur le réseau Internet, toujours par curiosité. En quelques jours, ce sont plus de 6000 machines qui vont ainsi être infectées, valant à Morris trois ans de mise à l'épreuve.

La curiosité est décidément un vilain défaut…

Outre son caractère anecdotique, l'arrestation de Morris est déterminante pour l'avenir des hackers, car il est une des premières victimes du Computer Fraud and Abuse Act, voté en 1986 par les Etats-Unis dans le but de lutter contre la délinquance informatique[167].

L'arrestation de Morris est également symptomatique de la fin du temps des pionniers. Internet et les réseaux informatiques deviennent les territoires de nouveaux aventuriers, parmi lesquels des criminels informatiques.

Le modem est devenu le meilleur ami du hacker, lui permettant ainsi de former des groupes, gangs, comme les Texans de la « Legion of Doom » (« Légion de mort/ruine/terreur »), les LoDs, dont le chef est « Eric Bloodaxe » (Hâche Sanglante), Chris Goggan de son vrai nom.

En 1990, ceux-ci dominent la Scène depuis six ans. Défiés par les New-Yorkais de « Masters of Deception » (« Maîtres de la tromperie »), les MoDs, ils vont se lancer une série de défis, toujours plus audacieux, à coups d'intrusions et autres piratages téléphoniques. Ce qui n'était qu'un jeu au départ va finalement dégénérer lorsque les MoDs vont s'infiltrer sur les ordinateurs de la société de sécurité informatique (!) Comsec, créée par les LoDs. Ceux-ci vont alors les dénoncer à la justice et les MoDs se verront condamner pour piratage informatique[168].

Au même moment, l'agitation provoquée par ces pirates des temps modernes devient mondiale.
En Allemagne, c'est le Chaos Computer Club qui va donner des sueurs froides aux responsables des systèmes informatiques[169] ; en France ce sont des étudiants de l'université de Jussieu qui s'infiltrent sur les machines de l'Ecole polytechnique ; en 1994, Vladimir Levin, mathématicien de Saint-Petersbourg s'introduit sur les réseaux de la Citybank et détourne 400.000$ avant de se faire arrêter et condamner à trois ans de prison ,…[170]

---

[167] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 13 et suiv.
[168] Nous y reviendrons plus tard.
[169] Nous y reviendrons plus tard.
[170] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 13 et suiv.

Les années 1990 vont ainsi voir la fin d'une ère et le début d'une nouvelle, la fin de l'ère des pionniers et l'apparition d'une véritable délinquance informatique ciblée, structurée.

Et surtout, les années 1990 verront l'explosion de la Scène.

Section 4 – Le conflit des générations

Au début des années 1990, le mot « hacker », qui était à l'origine dévolu aux artistes du clavier, est devenu, par glissement de sens, un terme générique désignant toute personne capable de s'immiscer dans un ordinateur. Il faut ajouter que dans la pratique, la majorité des médias n'étant pas au fait des subtilités du langage des hackers, le grand public croit surtout que les hackers sont exclusivement des délinquants, alors que, comme nous l'avons vu, il n'en est rien.

D'ailleurs, certains, à l'instar d'Eric Raymond[171], insistent sur les nuances lexicales, multipliant les définitions permettant de distinguer « hacker », « cracker », « lamer », « carder », « coder »,…

Mais, pour le grand public, comme nous venons de le dire, le hacker est avant tout un intrus, devenant tour à tour, au gré des discours, saboteur, renégat, cyberterroriste, soupçonné d'avoir des relations avec des états ennemis, les diverses mafia, d'être exclusivement motivé par le profit,… alors même qu'avec l'explosion des connexions à Internet dans le monde, une nouvelle génération monte sur la Scène, renforçant encore la panique ambiante[172].

L'immense majorité de ces apprentis pirates, souvent considérés avec mépris par les anciens, les premiers hackers de années 1960, se revendiquent d'un « hacking spirit » puisé dans l'histoire du genre, tout en y adjoignant une forte conscience de communauté.

A titre d'exemple, il nous suffit de dire que pendant les cinq années qu'il a passé en prison, le célèbre pirate Kevin Mitnick[173] a été considéré comme un véritable martyr par toute la Scène.

Des milliers de bannières « Free Kevin » ont ainsi orné les sites web de tous les apprentis pirates de la planète,… tout comme on pouvait les trouver sur les pages web des hackers les plus anciens[174].

---

[171] Eric RAYMOND est l'auteur du « Jargon File », texte célèbre sur le net relatif aux différents termes relatifs au monde des hackers. Il est disponible sur le site de l'auteur, à l'adresse www.tuxedo.org/~esr/.

[172] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 13 et suiv.

[173] Nous reviendrons plus en détails sur l'histoire et les « exploits » de Mitnick plus tard.

[174] Le plus célèbre de ces sites de soutien étant, bien entendu, www.freekevin.com.

A. LA GÉNÉRATION DES ANNÉES 1960 : LES HACKERS « OLD SCHOOL »

Comme nous l'avons vu, les premiers hackers commencèrent leurs activités au début des années 1960.

Leur recherche ininterrompue de nouvelles connaissances était alimentée par les découvertes des surdoués du Massachusstts Institute of Technology (MIT), dont un grand nombre de hackers respectés aujourd'hui sont issus.

Le MIT est fondamental pour comprendre l'esprit des hackers des années 1960. Il concrétise les aspirations des bidouilleurs de l'informatique d'alors, chacun rêvant de faire une découverte permettant de faire avancer le progrès informatique et chacun travaillant pour l'ensemble de la communauté.

La création d'Arpanet en 1969 a également eu des conséquences importantes pour ces surdoués de l'informatique.

Elle leur permet d'échanger leurs connaissances, leurs techniques, mais également de diffuser les fondements du « hacking spirit ». C'est à cette époque qu'apparaissent les premières listes de jargon (similaires à celle d'Eric Raymond dont nous reparlerons plus tard) – la première datant de 1973 –, ainsi que les première critiques, satires,…[175]

Avec la création d'Unix, une première rupture se fait. Les hackers en font leur propre environnement de travail ; et comme celui-ci possède son propre protocole réseau, les hackers constituent bientôt des réseaux dans le réseau.

Par la suite, la création du premier ordinateur personnel, en 1975[176], constituera une nouvelle rupture. Les hackers, après avoir privilégié l'échange, le partage, créeront des groupes, souvent rivaux.

Si le « hacking spirit » était quelque part respecté (la nécessité de dépasser, d'épater les autres groupes, obligeait les hackers à se surpasser et, partant, à faire de nouvelles découvertes), la rivalité entre groupes de hackers était désormais devenue une réalité, pourtant inimaginable vingt ans plutôt…

---

[175] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

[176] E., RAYMOND, « A brief history of Hackerdom », www.tuxedo.org/~esr/, 1999.

B. LES ANNÉES 1980 : LA RIVALITÉ DES HACKERS

Les années 1980 vont voir les hackers s'organiser en groupes de pression et commencer à se faire connaître du grand public.

Leurs revendications sont double : libertaires pour l'informatique, d'une part, et identitaires[177], d'autre part. Nous reviendrons plus tard sur l'importance de la notion de groupe lors de l'analyse de la théorie des associations différentielles de Sutherland.

Parmi l'ensemble de petites luttes intestines qui ont émaillé l'histoire de ces groupes de hackers, deux d'entre elles sont particulièrement à souligner.

La première, peut-être plus technique, oppose les défenseurs du système Unix de Berkeley aux versions proposées par la société AT&T. En clair, elle oppose les tenants de la « old school » et du « tout est gratuit » à ceux prônant un Unix commercial.

Plusieurs affiches de cette époque, faisant référence à la trilogie de « La guerre des étoiles », très prisée par les hackers, représentent ainsi un vaisseau de combat en forme de « X » fuyant une Etoile de la Mort symbolisant AT&T[178].

L'autre grande rivalité des années 1980 est celle opposant les LoDs aux MoDs[179]. Nous ne reviendrons pas ici sur les détails de leur querelle (nous les avons déjà abordés plus tôt), mais insisterons sur les caractéristiques de ces groupes.

Tout d'abord, le fait que les jeunes composant les LoDs étaient originaires du Sud des Etats-Unis, alors que les MoDs étaient New-Yorkais, ce qui incita certains à considérer cette querelle comme une vieille rivalité Nord/Sud. C'est mal connaître les hackers, du moins les hackers « purs »[180]. Ceux qui se qualifient ainsi visent le savoir avant tout, le but ultime étant de comprendre le fonctionnement de machines que l'on ne connaît pas.

Les deux groupes se revendiquaient de cette pensée, si bien que leurs actes, bien loin de simples actes de « racisme », étaient motivés par le défi, et que leur statut de criminels leur était conféré par le fait qu'ils pénétraient illégalement dans des systèmes informatiques, plus que par la nature de leurs actions, celles-ci n'étant que très rarement orientées vers la nuisance.

Il n'en demeure pas moins qu'une bonne partie de ces jeunes gens, qui n'avaient pour la plupart, conformément à leur idéologie[181], pas touché un sou de leurs activités, furent condamnés à des peines sévères[182].

---

[177] Voy. E., RAYMOND, « How to become an hacker ? », www.tuxedo.org/~esr/, 1999. Ce texte est reproduit en français en annexe.
[178] E., RAYMOND, « A brief history of Hackerdom », www.tuxedo.org/~esr/, 1999.
[179] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.
[180] E., RAYMOND, « A brief history of Hackerdom », www.tuxedo.org/~esr/, 1999.
[181] Nous y reviendrons plus tard.

Enfin, un autre groupe, le Chaos Computer Club[183] (CCC), mérite d'être mentionné. Les membres de cette organisation allemande, créée en 1981 et comptant plus d'un millier d'adhérents, sont guidés par le fondateur du Club, le «Dr Wau» (de son vrai nom Herwart Holland-Moritz). Celui-ci a conduit le groupe à commettre un nombre impressionnant de méfaits[184].

Le premier acte de piratage, datant de 1984, consistait en un détournement de fonds de la banque Sparkasse, détournement s'élevant à 100000 DM (en une seule nuit !). Mais, fidèle à l'esprit premier qui animait les hackers, l'argent fut restitué le lendemain matin. En 1987, c'est la NASA qui faisait les frais des démonstrations du CCC. Beaucoup d'autres suivront ensuite[185].

Les actions de ce groupe n'ont qu'un seul but : faire prendre conscience aux utilisateurs de la vulnérabilité de leurs systèmes informatiques. A cette «noble démarche », il nous faut ajouter le goût du risque, la fierté du défi réussi,… Quoiqu'il en soit, les hackers du CCC, comme les autres groupes « purs », n'ont pas l'impression d'être une menace pour la société et se revendiquent même comme étant les hackers «authentiques », allant jusqu'à se comparer à des chevaliers blancs menant une croisade pour une meilleure connaissance de la machine au service de l'Homme[186].

Peter Glaser, membre du Chaos Computer Club déclare d'ailleurs : *« L'Homme est au centre d'intérêt du CCC et non la machine »*[187].

Cette conception d'une «utilité sociale » du crime rejoint celle de Durkheim que nous avions déjà abordée. En effet, pour les hackers purs, le fait de s'introduire dans un ordinateur n'est pas un crime, mais, au contraire, vise à œuvrer pour le bien de l'Humanité, que ce soit en découvrant de nouvelles fonctionnalités, de nouvelles utilisations de leurs machines, ou en détectant les failles des systèmes de sécurité, permettant ainsi aux administrateurs d'apprendre à mieux protéger leurs systèmes informatiques.

---

[182] Les membres du MOD furent accusés de nombreux délits, parmi lesquels« Interception de conversations téléphoniques et de transmissions de données, possession de matériels et de logiciels d'intrusion, vol de mots de passe, vente de profils de crédit et destruction d'ordinateurs, pour un montant total de 370000$ ».

[183] Il est toujours en activité comme en témoigne son site web dont l'adresse est www.ccc.de.

[184] L'un de ses leaders, « Tron », a été assassiné (par la mafia ? par des services secrets ?), même si la version officielle de sa mort a longtemps été celle du suicide.

[185] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

[186] Nous reviendrons plus tard sur la notion d'éthique chez les hackers.

[187] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

C. LES ANNÉES 1990 : COMMUNAUTÉS VIRTUELLES ET HACKERS SOLITAIRES

Les années 1990 vont marquer un tournant dans la mesure où les groupes de hackers ont désormais tendance à s'institutionnaliser (par exemple le CCC), alors que de nombreux cas de hacking éclatent au grand jour (ces actes existaient déjà, mais étaient moins médiatisés).

Le groupe Electronic Frontier Foundation (EFF)[188] est tout à fait révélateur de cette tendance[189]. L'EFF fait partie de ces communautés virtuelles menant une croisade afin de préserver la liberté, la créativité, le bénévolat et le désordre qui caractérisent le réseau Internet.

Ce groupe doit sa création à l'arrestation infondée de Mitch Kapor et Perry Barlow[190]. Ils décidèrent tous deux de créer un organisme ayant pour mission de «civiliser le cyberespace » et d'éviter que des hackers ne soient arrêtés sans raison valable.

Leur première victoire (l'acquittement de Graig Niedorf) avait pour but d'établir une distinction fondamentale entre les diverses motivations des hackers : entre l'escroquerie, le vandalisme et l'exploit gratuit.

L'EFF connaîtra d'autres victoires, comme par exemple l'acquittement de Jake Baker, un étudiant qui avait été mis en prison pour avoir publié sur le réseau Internet des textes décrivant ses fantasmes sexuels.

Mais, du point de vue du grand public, ce ne sont pas les victoires du EFF qui seront marquantes, mais bien plutôt les exploits des nouveaux pirates[191]. Comment ne pas citer Kevin Mitnick, le hacker le plus recherché de la planète, ou Onel de Guzman et David L. Smith, respectivement créateurs des virus « *I Love You* » et « *Melissa* », ou, plus près de chez nous RedAttack ?

Les hackers des années 1990 présentent donc une disparité importante. Ce que nous en retiendrons surtout de cet historique sera est une querelle de légitimité entre les hackers « old school » des années 1960 majoritairement partisans du respect de la légalité d'un côté, et une nouvelle génération, confinée dans la clandestinité et n'hésitant pas à commettre des activités illégales.

---

[188] Le nom du groupe fait référence à la conquête de l'Ouest, un des éléments fondateurs des Etats-Unis.
[189] Cette partie consacrée au groupe EFF provient principalement de l'étude de documents disponibles sur le site-même du groupe, www.eff.com.
[190] Pour l'anecdote, Perry Barlow est, depuis 20 ans, le parolier du groupe de rock Grateful Dead.
[191] Les hackers célèbres et leurs motivations seront abordés plus tard.

Le célèbre congrès DefCon[192], tenu à Washington chaque année et rassemblant exclusivement des pirates (et des policiers se faisant passer pour tels), témoigne de l'agrandissement de ce fossé, les anciennes générations profitant de ces contacts pour affirmer leur volonté de s'inscrire dans la légalité et de coopérer avec les autorités[193].

Autre témoignage venant corroborer ce glissement, non plus vers la criminalité, mais désormais vers la légalité des hackers « old school », nous vient de Chris Goggan (le chef des LoDs), qui, au moment de quitter la Scène en 1996 déclarait : *« Je n'aime pas la plupart d'entre vous, les gars. La sub-culture des hackers est devenue une caricature de son passé (…). La communauté a dégénéré. C'est devenu une farce nourrie par les médias »*[194].

---

[192] Tirant son nom de « Defense Condition », le code utilisé par la défense américaine en cas d'attaque nucléaire, le premier congrès DefCona été organisé en 1993. Outre ses activités « officielles », il est également connu pour ses activités « off », parmi lesquelles *« Find the Fed »* (« identifiez l'agent du FBI ») ou encore *« Hack Party »* qui consiste en un piratage « live » et débridé.

[193] Toutes les informations concernant le congrès DefCon sont disponibles sur le site www.DefCon.com.

[194] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

Section 5 – Les hackers qui ont fait l'histoire

Lors de cet exposé, nous avons à plusieurs reprises évoqué le nom de hackers célèbres, sans entrer dans des détails très importants concernant leurs « exploits ».

Au vu de l'importance et l'ascendance qu'ils ont eues sur les nouvelles générations, il ne nous a pas semblé inutile de nous attarder quelques instants sur les plus importants et les plus déterminants d'entre eux.

Au sein de ce panthéon du hack, nous allons procéder à une distinction entre, d'une part, les « gourous » (ou hackers « old school »), et, d'autre part, les cybercriminels.

A. LES GOUROUS

1) Richard Stallman

Richard Stallman est le fondateur d'un projet lancé en 1984 et ayant pour objet le développement d'un système d'exploitation gratuit. Ce projet, le GNU[195], devait rendre aux utilisateurs une liberté qu'ils avaient pour la plupart perdue[196].

Le manque de liberté décrit par Stallman a une double cause. Tout d'abord, les logiciels commerciaux étant les seuls à être développés de manière professionnelle, les consommateurs sont obligés de dépenser des sommes plus ou moins importantes afin d'utiliser des produits de qualité (le problème étant que, généralement, le prix de ces logiciels est très élevé). Le fait d'acheter ces logiciels est donc considéré par Stallman comme une obligation et non un choix.

Ensuite, les codes sources de ces programmes ne sont (quasiment) jamais fournis avec les programmes, si bien que les consommateurs n'ont aucune possibilité de modifier, d'adapter les logiciels qu'ils ont achetés selon leurs besoins.

Le projet de Stallman vise donc la totale gratuité des logiciels, ainsi que le droit pour chaque utilisateur de copier, distribuer et modifier ces logiciels[197].

Le projet de Richard Stallman est le fruit d'un besoin de liberté exacerbé par son passage au MIT. Stallman s'y sent enfermé, coincé, ne supporte pas que la culture de compétition, des secrets de fabrication l'emporte sur sa passion première. Stallman déclare d'ailleurs que *« les hackers cassaient occasionnellement la sécurité des ordinateurs. Celle-ci était mise en place par les administrateurs pour contrôler les utilisateurs, les surveiller. Et les hackers ont peu de respect pour la bureaucratie »*[198].

---

[195] « GNU » est l'acronyme récursif de « GNU's Not Unix ».
[196] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 24 et suiv.
[197] Pour de plus amples détails, nous renvoyons au site de GNU dont l'adresse est www.gnu.org.
[198] Richard Stallman possède son propre site dont l'adresse est www.stallman.org.

Stallman finira par quitter son poste au milieu des années 80 et dirige aujourd'hui une société, la « Free Software Foundation » développant des logiciels gratuits, et, il insiste, *« de qualité »*[199].

2) Denis Ritchie et Ken Thompson

Ces deux gourous sont à l'origine du système Unix en 1969[200].

Unix a été déterminant pour les hackers car il leur a permis de développer plus facilement, et avec plus de possibilités, leurs propres applications, leur permettant ainsi d'approfondir leurs connaissances.

Unix a connu plusieurs variantes et a été porté sur la plupart des ordinateurs, de l'ordinateur central au PC à processeur Intel, touchant ainsi des centaines de milliers d'utilisateurs.

L'actuelle variante de Unix est aujourd'hui « Linux », qui est un système d'exploitation complètement gratuit (et le principal concurrent du « Windows » de Microsoft)[201].

3) Steve Wozniak et Steve Jobs

Comme nous l'avons déjà évoqué, Steve Wozniak et Steve Jobs sont les fondateurs de la société Apple et du Macinstosh.

Anciens phreakers et membres du *« Homebrew Computer Club »* de Menlo Park en Californie[202], Wozniak et Jobs se sont rapidement démarqués des autres hackers. Tout d'abord, par la production massive de blue boxes, et ensuite par le lancement de la société Apple dans le garage parental.

Lorsqu'ils lancèrent leur premier micro-ordinateur, le Apple II, en avril 1977, leur slogan était *« Power to the people »*, avec pour ambition de donner accès à chacun à des outils de traitement de l'information, auparavant réservés aux entreprises et aux gouvernements[203].

Rien qu'avec ce slogan, Jobs et Wozniak marquèrent clairement leur appartenance aux hackers « purs », old school, la blue boxe et Apple leur permettant de rentrer définitivement dans l'histoire.

---

[199] Voy. le site de Richard Stallman, www.stallman.org.
[200] Y., CHATELAIN, L., ROCHE, Marketing et cybecriminalité, Paris, Hermès, 2000, pp. 54 à 59.
[201] Le site du système d'exploitation « Linux» est www.linux.org.
[202] Créé en 1975, ce club avait pour objectif de favoriser le développement des micro-ordinateurs et de démocratiser l'accès à l'informatique.
[203] D., LABROSSE, « Hackers, la cyberculture à ses extrêmes », http://www.er.uqam.ca, 2001.

B. LES CYBERCRIMINELS

1) Kevin Poulsen

Surnommé « Dark Dante », Kevin Poulsen était spécialisé dans le piratage de systèmes gouvernementaux et militaires. Ses « exploits » lui avaient d'ailleurs permis de devenir consultant pour le ministère de la Défense au Pentagone.

Loin d'arrêter ses activités criminelles la nuit, Poulsen était un employé modèle le jour. Il fut ainsi accusé, entre autres, de conspiration, de fraudes, d'écoutes téléphoniques, de blanchiment d'argent.

En 1990, il prit le contrôle des 25 lignes téléphoniques d'une station radio de Los Angeles, afin de ne laisser filtrer que ses appels. Il put ainsi être le 102ème appel, gagnant par la même occasion une Porsche 944 d'une valeur de 50000$.

Condamné le 10 avril 1995, il fera 51 mois de prison[204].

2) Kevin Mitnick

Lorsqu'il était adolescent, une des blagues favorites du futur « Condor » consistait à détourner les appels au service de l'annuaire vers son domicile[205]. Un abonné pouvait donc se trouver devant une situation de ce type :

- *Abonné : Bonjour, je voudrais le numéro de M. X s'il vous plaît.*
- *Mitnick : Bien sûr, un moment… Euh, Monsieur X est-il blanc ou noir ?*
- *Abonné : Pourquoi ?*
- *Mitnick : Voyez-vous, chez AT&T, nous avons deux types d'annuaire : un pour les blancs et un pour les noirs…*

Contrairement à la majorité des hackers, Kevin Mitnick n'avait pas véritablement d'idéologie[206].

Il s'est fait la main en surveillant discrètement les e-mails des fonctionnaires américains en charge de la sécurité informatique sur le territoire des Etats-Unis.

En 1989, Mitnick, âgé d'une vingtaine d'années, réalise son premier hack d'importance. Il réussit à subtiliser un nouveau système d'exploitation (le VMS-OS) dont la valeur était alors de 1 million $.

Ensuite, autre hack d'exception, il réussit à s'introduire dans la base de données du « California Department of Motor Vehicules » et y subtilise plus de 20000 numéros de cartes bancaires.

---

[204] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

[205] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, p. 27.

[206] Nous y reviendrons plus tard.

Il se fera arrêter une première fois, après avoir échappé à la police pendant plusieurs années en piratant et espionnant les conversations téléphoniques et les mails de ses poursuivants. Pris en flagrant délit alors qu'il s'infiltrait sur les ordinateurs du haut commandement de l'US Air Force, il expliquera au juge qu'il désirait simplement faire une bonne blague[207].

Condamné ainsi une première fois à une peine de prison, à peine sorti il récidivera, dérobant cette fois pour un million $ de logiciels à une société informatique, toujours « pour rire ». Visiblement, le FBI n'avait pas le même humour que Kevin, et fera de lui le premier hacker à intégrer la célèbre liste des « Most Wanted Criminals » (les criminels les plus recherchés).

Après plusieurs mois de prison, il récidivera encore une fois, et à nouveau, se fera prendre, cette fois par un hacker repenti désormais au service du FBI, Tsutumu Shimomura[208].

Après une cavale de plusieurs mois, Mitnick sera arrêté et incarcéré au pénitencier de Los Angeles dont il ne sortira que cinq ans plus tard.

Il restera en outre en liberté surveillée jusqu'en 2003, avec l'interdiction de se servir du plus petit ordinateur comme des téléphones portables, l'idée étant de lui interdire tout contact avec du matériel lui permettant d'accéder à un réseau informatique.

Dans le même temps, comme souvent avec les anciens hackers, il fera l'objet de diverses invitations devant le gouvernement américain, afin de demander, un jour devant le Sénat, un jour devant une commission spécialisée, la mise en place de systèmes de détection et de prévention efficaces afin d'assurer la sécurité des réseaux… ainsi qu'une relative clémence contre les pirates informatiques.[209]

Quelque soit son avenir, l'histoire de Kevin Mitnick est déjà entrée dans la légende. Les mesures exceptionnelles dont il fait l'objet n'y sont pas étrangères, John Markoff (co-auteur de *Cybertraque*) comparant même Mitnick à Hannibal Lecter, le psychiatre psychotique du roman de Thomas Harris, *Le Silence des agneaux*, et dont les mains devaient être liées pour éviter un accident majeur, cet accident majeur pouvant être, dans le cas de Mitnick, la destruction d'Internet[210].

---

[207] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 20 et Suiv.
[208] Voy. T., SHIMOMURA, J., MARKOFF, *Cybertraque – La chasse au pirate informatique le plus célèbre des Etats-Unis*, Paris, Plon, 1998.
[209] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 28 et suiv.
[210] E., RICHARD, « Hacker brisé », Libération, mardi 14 mars 2000.

Section 6 – Les faits marquants de l'histoire de la criminalité informatique

Afin d'être tout à fait complet, il nous semblait intéressant d'aborder ce qui nous paraît être un complément indispensable à notre historique sur la criminalité informatique.

Nous avons reproduit en annexe, chronologiquement, les faits les plus marquants et relatifs à l'informatique en général, et à la cybercriminalité en particulier[211].

Nous constaterons ainsi que plus l'on s'approche des années 1990 et plus le nombre de faits augmente, nous permettant ainsi de souligner que ce sont bien les années 1990 qui ont véritablement vu l'explosion de l'informatique, et donc, des hackers (au grand jour d'une part, et en plusieurs groupes rivaux d'autre part).

Enfin, il sera intéressant pour chacun de constater que certains de ces éléments nous sont connus, ont été relatés, commentés dans les médias, … et que ces éléments sont généralement de nature criminelle.

C'est ce type de faits qui sera véritablement à la base de la prise de conscience par le grand public et le monde politique et judiciaire du phénomène du piratage informatique et surtout de l'ampleur des dégâts que ce type de criminalité peut causer, et qui amèneront les gouvernements à prendre les mesures nécessaires, comme cela a, par exemple, été le cas pour la Belgique avec la nouvelle loi du 28 novembre 2000 relative à la criminalité informatique.

[211] Pour cette partie, notre source principale a été le site de Symantec, leader mondial dans le domaine des logiciels de sécurité, dont l'une des adresses est www.symantec.fr, et qui publie une série d'informations sur l'ensemble des domaines relatifs à l'informatique et à l'utilisation qui peut en être faite.

Conclusion quant à l'historique du hacking

Cet historique du hacking nous a donc appris que les hackers n'étaient pas au début, du moins la majorité d'entre eux, les cybercriminels que beaucoup sont devenus aujourd'hui.

C'est l'association des phreakers et des hackers qui a permis à chacun de dépasser ses limites, certains dépassant celles imposées par la loi.

A partir de là, si « l'esprit du hack » avait animé les premiers hackers, les hackers « purs », c'est désormais bien souvent « l'esprit du lucre » qui anime les nouveaux hackers des années 90, les « crackers ».

La genèse des différents groupes ayant été dressée, il est temps désormais de nous intéresser aux différentes caractéristiques des hackers.

Titre II – Les caractéristiques des hackers

La culture des hackers, leur mode de vie, leurs motivations,… ont fait l'objet de beaucoup d'ouvrages. A l'analyse de ceux-ci[212], il nous sembla indispensable de poser la question directement aux principaux concernés. Après quelques clics sur le Net, nous avons trouvé cet exposé du célèbre hacker Eric S. Raymond, qui nous explique « comment devenir un hacker »[213].

La lecture de ce document nous permet déjà d'avoir une certaine idée de la culture des hackers et des hackers eux-mêmes.

Il semblerait tout d'abord que, de par l'existence-même de ce document, beaucoup de gens veulent devenir des hackers.

C'est pour nous l'occasion de nous pencher sur une caractéristique essentielle des hackers, à savoir que ce sont les seuls criminels à publier des documents, des manifestes, des guides, … relatifs à leurs activités.

Certes, il existe des manuels pour parfaits terroristes, expliquant comment faire des bombes et autres cocktails molotovs, des fichiers expliquant comment réaliser des passe-partout, … mais pas en aussi grande quantité que ceux relatifs au hacking[214].

Selon l'auteur, *« les hackers ont créé l'Internet »*. Même si ceci est complètement faux[215], il n'en reste pas moins l'idée que les hackers font partie du paysage informatique, qu'ils sont inévitables.

Ceci s'explique notamment par la fascination suscitée par les faits dont les hackers sont responsables. Si certains sourient devant l'ingéniosité dont les pirates sont capables, devant les détournements amusants de sites Internet, trouveraient-ils aussi amusant un terroriste réalisant une « petite » bombe « pour rire », un voleur cambriolant une « petite » maison ?

Il n'est pas simple de se positionner vis-à-vis du hacking. Comparer une bombe à un détournement de site Internet tient évidemment un peu de la provocation, mais permet néanmoins bien de poser le problème que constitue le phénomène du hacking et les dégâts qu'il peut occasionner.

Ensuite, si l'on en croit l'auteur, les hackers forment une communauté, légèrement mégalomaniaque, ayant des centres d'intérêts variés (les arts martiaux, le Zen…), aimant les bons mots, défendant la liberté, réfractaires à toute autorité ainsi que vis-à-vis de la censure et du secret, cherchant l'accomplissement intellectuel, aimant avant tout donner et partager,…

---

[212] Nous développerons cette analyse plus tard.

[213] E., RAYMOND, « How to become an hacker ? », www.tuxedo.org/~esr/, 1999. Ce texte est reproduit en français en annexe.

[214] Pour s'en convaincre, il suffit de taper « hacking » dans n'importe quel moteur de recherche, ou encore de consulter des sites spécialisés, tel http://astalavista.box.sk.

[215] Voir la partie consacrée à l'historique du réseau Internet abordée précédemment.

Cette manière de considérer les hackers ne s'applique qu'à une certaine catégorie, et non pas à l'ensemble d'entre eux.

Il est ainsi important de souligner que les pirates informatiques n'ont en commun avec les hackers « purs » qu'une passion réelle pour l'informatique. Mais si les uns voient là une possibilité de contribuer au bien de la communauté, voire de l'Humanité parfois, les autres ne visent qu'un seul profit : le leur.

Car si les hackers sont tout ce qui vient d'être évoqué, ils ne s réduisent pas à cela, comme nous allons le voir à présent.

Cette partie relative aux caractéristiques des hackers sera divisée en trois sections.

Dans la première section, nous aborderons les subtilités de langage distinguant les différentes catégories de hackers, soulignant ainsi qu'il n'est pas nécessaire d'être très doué pour être un hacker.

La deuxième section sera consacrée aux fondements idéologiques du mouvement hacker.

Nous aborderons ainsi la culture des hackers, évoquant le cyberpunk, la TAZ ou encore l'underground.

Ensuite, c'est l'appréciation des hackers vis-à-vis des médias et par les médias qui sera analysée.

Enfin, nous terminerons cette section par l'éthique des hackers, ce qui sera pour nous l'occasion d'appliquer au monde des hackers les théories criminologiques développées par Sutherland et Sellin.

La troisième et dernière section sera principalement consacrée à l'analyse des motivations des hackers, ce qui nous amènera à évoquer les théories de Becker et de Merton.

Section 1 – Hackers, crackers, lamers,…

Comme nous l'avons déjà dit à plusieurs reprises, les histoires, anecdotes d'intrusion dans des systèmes sont de plus en plus fréquentes, les médias décrivant les hackers comme des génies pouvant s'introduire dans n'importe quel système et capables d'à peu près n'importe quelle prouesse technique.

Ce serait avoir une vision plus qu'irréaliste des hackers, car tous ne sont pas aussi ingénieux que l'on pourrait le croire.

Ainsi, ce n'est pas tant le génie informatique, scientifique qui distingue les hackers que la persévérance et l'effort dans l'apprentissage du hacking, ainsi que l'usage qui est fait de cet apprentissage.

A. LE HACKER

Comme nous l'avons vu, le hacker n'est au départ qu'un simple «bidouilleur », un passionné d'informatique. Les hackers ne sont pas tous des criminels, la majorité s'introduisant dans les systèmes par jeu, défi, ou pour accroître leurs connaissances[216].

Au sein de la Scène, il existe une hiérarchie établie selon plusieurs critères, dont les principaux sont les méthodes d'apprentissage du hacking et l'usage qui en est fait, et non, comme nous pourrions le penser, la médiatisation de leurs « exploits ».

Les hackers véritables insistent d'ailleurs bien sur le fait que ce n'est en aucun cas les médias qui font de vous un hacker, mais seulement la reconnaissance de pairs. Cette reconnaissance sera le fruit d'apprentissage, de conformité aux normes édictées par la communauté des hackers, à ses idées,… Dès lors, dans le cas des hackers «purs » (on ne vise pas ici les cybercriminels), l'entrée dans l'illégalité ne sera que la conséquence d'une interprétation défavorable de la loi par rapport aux buts poursuivis par le groupe. Sutherland, comme nous le verrons plus tard, a décrit ce concept, qu'il appelle la théorie des associations différentielles.

1) Les Curious Joe

Comme leur nom l'indique, ce sont des personnes très curieuses du hacking et ayant assez de connaissances pour causer des dégâts. Leurs vecteurs d'apprentissage sont les forums, les sites FTP. Leurs principales activités consistent à tester leurs trouvailles, et ce, sans intention foncièrement mauvaise[217].

---

[216] Nous renvoyons aux parties précédentes pour de plus amples informations sur ce qu'est un hacker.
[217] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp.67 et suiv.

2) Les Script Kiddies et les Lamers

• Les **Script-kiddies**[218] sont le plus souvent des néophytes en matière d'informatique. Ils ont pour objectif de nuire, avec plus ou moins d'intensité, avec des programmes trouvés sur des sites comme astalavista.box.sk, qui fournit des programmes de hack prêts à l'emploi, accompagnés de toutes les explications nécessaires.

Le rapport effort/plaisir est très intéressant pour eux, ce qui aurait tendance à leur donner un sentiment de puissance, mais ils sont en réalité méprisés par les véritables hackers en raison de leur manque de compétences réelles en informatique et de leur éloignement vis-à-vis de «l'esprit du hack »[219].

Parmi les hacks les plus fréquemment opérés par les script-kiddies, nous trouvons le « deface »[220].

Le deface consiste en la modification d'une page d'un site Internet, en général de la page d'accueil , et permet aux script-kiddies de « faire un coup », de se faire connaître, sans trop d'effort.

Comme de nombreux faits de hacking, le deface fait rarement l'objet de plaintes et de poursuites. Plusieurs raisons, propres au «deface », expliquent cet état de fait, en plus de celles précédemment évoquées lors de l'analyse du chiffre noir :

- Pour un administrateur de site Internet, faire état d'une intrusion, c'est reconnaître une forme d'incompétence.
- En l'absence de réactions de sa part, l'administrateur peut espérer voir les defacers s'attaquer à d'autres cibles, et éviter également de devenir la cible de groupes de «crashers » (de destructeurs de sites).
- Nous pouvons également y voir une volonté de dissimuler ces mésaventures à la presse, et d'éviter ainsi d'effrayer les actionnaires éventuels.
- Enfin, les administrateurs préfèrent parfois ne pas porter plainte et prendre connaissance des failles mises à jour par les hackers.

Ainsi, lorsqu'on demande à « Asmodeus », l'un des leaders de la « Belgian Hacker Zone »[221], s'ils sont souvent contactés par les administrateurs, il déclare : «*Nous sommes contactés au moins une fois sur deux. Les webmasters qui prennent contact ne portent jamais plainte. Nous leur expliquons quelle faille a été utilisée et comment ils peuvent la corriger pour éviter d'autres attaques. Le plus souvent, ils suivent nos recommandations »*[222].

---

[218] Il s'agit d'un néologisme faisant référence au « script », c'est-à-dire à l'écriture de programmes informatiques, et de « kid » qui fait référence au monde de l'enfance.

[219] Voy. le site consacré à la cybercriminalité et réalisé dans le cadre de la conférence NTIC de l'IEP Paris en 2000-2001, www.ifrance.com/cybercrime.

[220] Ce qui ne veut pas dire qu'il soit exclusivement exécuté par des script-kiddies.

[221] Il s'agit ici de hackers, et non de simples script-kiddies.

[222] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, p. 98.

• Les **Lamers**, quant à eux, sont encore moins compétents que les script-kiddies. Leur seule différence vient du fait que si les script-kiddies utilisent des programmes créés par d'autres et ont ainsi la possibilité de se faire connaître par leurs actions, les lamers ont en revanche la réputation de se vanter d'exploits qu'ils n'ont jamais accomplis.

3) Les Wannabes

Littéralement les « Je veux être », ils constituent les hackers en devenir. Généralement, ils commencent par améliorer des scripts existants, ce qui les distingue des script-kiddies et leur vaut une certaine approbation des véritables hackers (pour autant qu'ils restent dans la légalité). Lorsqu'ils auront développé leurs propres scripts, ils atteindront leurs objectifs et deviendront des « Elites »[223].

4) Les Elites

Ce sont, comme on l'imagine, les hackers véritables, les plus doués. Véritables exemples pour les autres catégories, mis à part peut-être pour certains script-kiddies, ils se subdivisent en plusieurs sous-groupes :

• **Les « Whites Hats » :**

Ce sont généralement des consultants en sécurité, des administrateurs réseaux, ou encore des cyberpoliciers. Ayant un grand sens de l'éthique et de l'esprit du hack originel, ils apprécient dans le hacking un subtil mélange de jeu, de défi et de fierté.

Ce sont probablement les plus proches de «l'idéologie hacker », se donnant souvent pour mission de défendre la liberté d'expression et le libre partage des connaissances.

Leurs positions amènent parfois certains d'entre eux à s'opposer farouchement aux bureaucrates, aux hommes d'affaires désireux de considérer le Net comme une simple entreprise commerciale, ce qui les fait parfois se transformer en « Grey Hats »[224].

• **Les « Grey Hats » :**

Ce sont des Elites ayant une position intermédiaire, ne rechignant pas à s'introduire dans un système, mais refusant de céder ou de promouvoir l'anarchie.

• **Les « Blacks Hats » :**

Vivant généralement dans la clandestinité, ils sont largement rejetés par les autres hackers en raison de leurs activités franchement illégales : espionnage, escroquerie, vandalisme, propagation de virus, cyberterrorisme, destruction de sites,…[225]

---

[223] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 67 et suiv.
[224] Y., EUDES, « Au bonheur des pirates », Le Monde, jeudi 26 octobre 2000.

Ils sont souvent les hackers les plus connus des médias et du grand public, alors que les hackers « purs » ne les considèrent pas comme faisant partie des leurs, notamment parce qu'ils ne respectent pas « l'esprit du hack »[226].

5) Les Corsaires

Les corsaires ne s'intègrent pas véritablement dans la hiérarchie qui vient d'être établie. Ce sont des hackers, de tous niveaux, ayant choisi d'aider ou de rejoindre les services luttant contre la criminalité des réseaux[227].

Il s'agit par exemple de formateurs d'agents de l'Etat, d'anciens hackers repentis,…

On peut les comparer aux Whites Hats, à ceci près que ces derniers exécutent encore des hacks par jeu, par défi, alors que les corsaires se cantonnent à contribuer à la lutte contre la criminalité.

Pour conclure cette partie consacrée aux différentes catégories de hackers, nous proposons ici un extrait de l'interview de « Big Jim », qui confirme ce qui vient d'être dit précédemment, notamment en ce qui concerne l'éthique des hackers et les rivalités qui les opposent. Ainsi, à la question « cela veut dire quoi être un hacker ? », il répond : *« Avant tout, lutter pour une libre communication. C'est vouloir rester dans un monde qui nous plaît; pouvoir acheter du pain sans être tracé ou fiché. L'idée d'un espace ouvert et communautaire comme le définit le CCC (Chaos Computer Club) allemand est la doctrine à laquelle je crois »* [228].

---

[225] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 67 et suiv.
[226] Nous reviendrons plus tard sur ce concept.
[227] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 75 et suiv.
[228] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 93 à 94.

B. LE CRACKER

Surnommé « dark-side » hacker par les hackers véritables, faisant ainsi référence au film Star Wars[229] et au « côté obscur de la Force », le cracker est un hacker qui tire parti de ses compétences informatiques en vue d'en retirer un bénéfice financier ou dans le but de nuire à des individus ou des organisations.

Hermétiques à «l'esprit du hack », les crackers opèrent dans de nombreux milieux et pour de nombreuses personnes. Ils peuvent travailler seuls ou en groupe, réaliser des objectifs personnels ou exécuter des « commandes » (ils travaillent pour la mafia russe, les cartels de la drogue, exécutent des actions de cyberterrorisme, de cyberespionnage…)[230].

Les Blacks Hats se différencient des crackers car ceux-ci sont spécialisés dans le « crack », c'est à dire la destruction, le cassage de codes de sécurité, de mots de passe, bien que la plupart d'entre eux ne se limitent pas à cette forme de hacking.

Ils sont évidemment détestés par la plupart des hackers.

C. LE PHREAKER

Comme nous l'avons vu, le phreaker est un spécialiste du piratage des télécommunications. Son activité peut être criminelle ou non.

Beaucoup de vrais hackers ont été des phreakers afin de diminuer le montant de leur facture téléphonique et pouvoir ainsi continuer leurs expérimentations et maintenir le contact avec les autres hackers.

L'émergence d'Internet et la baisse des coûts de communications a partiellement réglé le problème, les phreakers s'étant «reconvertis » dans le piratage des cabines téléphoniques ou des téléphones mobiles par exemple.

D. LES CYPHER PUNKS, LES CRASHERS ET LES AUTRES

Enfin, certains hackers, criminels ou non, se spécialisent dans certains types de hacks. Parmi les plus connus, citons les Cypher Punks qui sont ainsi les experts en chiffrement (cryptage, décryptage de données), les crashers qui cherchent à détruire les données des ordinateurs infiltrés, les carders qui sont des experts dans le domaine des cartes à puces et les coders dans tout ce qui concerne les codes (de sécurité le plus souvent)[231].

---

[229] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

[230] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 74 et suiv.

[231] Voy. le site consacré à la cybercriminalité et réalisé dans le cadre de la conférence NTIC de l'IEP Paris en 2000-2001, www.ifrance.com/cybercrime.

E. CONCLUSION

A titre de conclusion, il nous faut tout d'abord pointer que ces catégories sont le fait des hackers eux-mêmes et qu'ils sont parfois les seuls à cerner les différentes nuances entre chacune d'elles. Le néophyte aura en effet quelque mal à déterminer, à la seule lecture d'un crime informatique, si celui-ci est le fait d'un Black Hat, d'un Wannabee ou d'un cracker par exemple.

Ces catégories sont également l'occasion de souligner, contrairement à une idée préconçue, qu'il n'est pas nécessaire d'être un informaticien particulièrement doué pour être un pirate informatique, les script-kiddies et les lamers en étant la parfaite illustration.

Au niveau de l'application de la loi, ces catégories n'ont pas d'influence, les hackers étant punis de la même manière, quel que soit leur « niveau ».

Par contre, cette classification a une importance capitale pour les hackers, leur permettant de structurer la Scène, la faisant reposer sur une hiérarchie établie de manière « objective », sur base de leurs actions. Elle leur permet de s'identifier véritablement à une communauté, ayant ses règles et sa hiérarchie, ses buts et ses besoins, créant ainsi un véritable sentiment d'appartenance. C'est un élément important, Sutherland y voyant même, comme nous le verrons un peu plus tard, l'une des explications au comportement délinquant.

Section 2 – Culture, idéologie et éthique du hacker

Nous allons ici aborder ce qui constitue l'univers au sens large des hackers. Comme de nombreux groupes, les hackers se sont forgés une histoire, des codes, un langage,… qui vont structurer leur communauté, la solidifier, voire la justifier.

A. LA CULTURE CYBERPUNK ET LE CYBERESPACE

Dans son roman *Neuromancer*, William Gibson décrit un monde où se réalise l'alliage étrange du biologique et du technique. La technologie s'intègre directement au corps humain, comme un implant, faisant partie de sa chair[232].

Le roman de Gibson est essentiel pour les hackers, et ce, pour deux raisons.

Tout d'abord, C'est dans «Neuromancer » que Gibson va forger le terme «cyberespace »[233]. Cette expression ne connaît pas de définition précise et c'est sans doute pourquoi elle convient tant à ceux qui l'emploient désormais pour désigner l'espace sans frontières d'informations qu'est l'Internet.

Cette expression a été adoptée au moment de la création des navigateurs Web, comme « Gopher » qui permettait aux apprentis surfeurs de trouver, de naviguer parmi les milliers d'informations du Net. Alors qu'avant 1992, le réseau Internet était principalement le fief des universitaires, des militaires et des spécialistes des télécommunications, avec Gopher et l'avènement du cyberespace, l'Internet s'ouvrait aux néophytes[234].

Ensuite, « Neuromancer » est un des documents fondateurs de la culture «Cyberpunk »[235]. Le terme « cyberpunk » est formé de deux composantes :

- « cyber », qui désigne la « cybernétique » (l'art de gouverner) et, partant, les nouvelles technologies associées à l'informatique.
- « punk », qui renvoie au mouvement de contre-culture du même nom.

---

[232] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

[233] Gibson avait déjà inventé ce terme en 1981, mais ce n'est qu'avec « Neuromancer » que celui-ci prendra de l'importance, Gibson l'utilisant à plusieurs reprises.

[234] L., CASTANY, A., FAUVEL, J., HARDOUIN, « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999. Ce site a été réalisé dans le cadre de la conférence sur les NTIC de Sciences-Po Paris.

[235] En réalité, le terme « cyberpunk » a été inventé en 1984 par Gardner Dozois, directeur de la revue de science fiction Asimov SF Magazine, pour désigner un nouveau courant de la science-fiction qu'il avait d'abord appelée « Punk SF ».

La culture cyberpunk renvoie d'une part à un mouvement littéraire, artistique et cinématographique (avec par exemple, des films comme « Blade Runner », ou plus récemment « The Matrix »), et d'autre part, à une contre-culture[236].

Cette contre-culture, si elle est inspirée de celle du mouvement« punk », n'en est pas moins différente sur un point essentiel.

Pour les punks des années 70, les nouvelles technologies associées à l'informatique sont aliénantes. Ils n'ont aucun espoir dans le futur de l'humanité (d'où la célèbre expression « No Future ! »), et ils utilisent leur corps comme « outil de communication », de manière provocatrice, au moyen du « piercing »[237].

Pour les cyberpunks, par contre, les nouvelles technologies sont libératrices, portent en elles un espoir de progrès pour l'Homme, et donc, de futur.

Cette transformation du pessimisme punk en optimisme cyberpunk sera le fruit des ouvrages de Gibson, Sterling, et d'autres écrivains de la même mouvance[238].

La culture cyberpunk se réfère au mouvement de contestation et de révolte des années 1970, regroupant principalement de jeunes anarchistes. Mais à la différence du punk traditionnel, le cyberpunk s'avère être particulièrement doué pour les nouvelles technologies. Anarchiste lui aussi, il entend utiliser ses compétences dans sa lutte contre le Système.

Ces auteurs vont faire du mouvement cyberpunk un mouvement de contre-culture, où les nouvelles technologies ne serviront pas à asservir l'Homme ou à l'exploiter (sur le plan commercial notamment), mais au contraire, à l'affranchir de ses servitudes et ainsi œuvrer au bien de l'Humanité[239].

L'information comme élément de libération est un des thèmes récurrents chez les hackers. Ceux-ci ne cessent de revendiquer un Internet libre, qui ne ferait pas l'objet d'enjeux commerciaux, et d'une manière générale, un accès libre à tout type d'informations.

Dès lors, il était inévitable que de nombreux hackers se réclament du mouvement cyberpunk, s'identifiant à « Case », le cow-boy du cyberespace de Gibson qui réussit à s'infiltrer dans les systèmes les plus sécurisés[240].

---

[236] G., LAPASSADE, « Qu'est-ce que le cyberpunk ? Littérature et contre-culture », www.ai.univ-paris8.fr/corpus/lapassade/cyberpun.htm, 1993.

[237] Cette pratique est directement en relation avec les implants « technologiques » évoqués dans les romans cyberpunk

[238] G., LAPASSADE, « Qu'est-ce que le cyberpunk ? Littérature et contre-culture », www.ai.univ-paris8.fr/corpus/lapassade/cyberpun.htm, 1993.

[239] C'est par exemple le cas dans le film « The Matrix » où Néo, après avoir été l'esclave de la « Matrice », va devenir l'espoir de l'Humanité et se battre pour que celle-ci retrouve sa liberté, ses alliés n'étant ni plus ni moins que des hackers confirmés.

[240] Il existe divers textes, écrits par des cyberpunks, commentant et expliquant ce qu'est la culture cyberpunk et ce qu'elle représente, et facilement disponibles sur le Net. A titre d'exemple, nous renvoyons au texte *« Pourquoi le Cyberpunk ? »*, publié en annexe.

Cette rupture avec l'Etat, et avec toute institution centralisée, rapproche, de facto, les hackers des mouvements anarchistes et libertaires.

Néanmoins, il manquait encore un jalon pour les lier. Ce chaînon manquant, c'est la TAZ, ou Temporary Autonomous Zone. Pour bien comprendre ce qu'est la TAZ, il nous faut d'abord parler de l'idéologie des hackers.

B. L'IDÉOLOGIE DES HACKERS

Comme nous l'avons déjà évoqué, l'idéologie des hackers est basée sur le principe que toute information doit être libre et que l'accès aux ordinateurs doit être illimité et total[241].

Fondamentalement, cette idéologie repose sur quatre points communs à tous les hackers (purs) :

1°) Contrairement aux crackers, les hackers cherchent à « construire quelque chose »[242].

2°) Ce n'est ni la presse, ni l'auto-proclamation qui fait de vous un hacker, mais exclusivement la Scène, la communauté du hack.

3°) Les hackers s'accordent sur ce qui constitue un bon « hack ». Celui-ci doit être simple, doit faire preuve d'une véritable expertise technique, doit être illégal et ne doit pas être limité aux seules intrusions sur ordinateur.

4°) Tous doivent adhérer à « l'esprit du hack ». Celui-ci va clairement distinguer les hackers des crackers et des cyberterroristes. L'esprit du hack sous-tend une série de valeurs que les hackers se doivent de défendre :

- la gratuité de l'information sur le réseau Internet ;
- la propriété intellectuelle doit appartenir à tous ceux qui en ont la compréhension ;
- les grandes entreprises ne sont pas dignes de confiance ;
- les grands gouvernements encore moins ;
- toute tentative de légiférer et donc de restreindre le cyberespace doit être combattue ;
- le savoir-faire technique est la vertu qui doit être la plus valorisée[243] ;

Pour bien cerner ce qui fonde l'esprit du hack, il nous faut nous intéresser à la TAZ.

---

[241] S., LEVY, *Hackers : heroes of the Computer Revolution*, New York, Delta, 1984, p. 40.

[242] E., RAYMOND, « How to become an hacker ? », www.tuxedo.org/~esr/, 1999. Ce texte est reproduit en français en annexe.

[243] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 49 et suiv.

1) La Temporary Anonymous Zone

Le rôle de la Temporary Anonymous Zone (TAZ) est déterminant. D'une part, elle va jouer le lien entre le mouvement cyberpunk et l'idéologie des hackers, et, d'autre part, elle va constituer le fondement de ce qui deviendra l'esprit du hack.

En 1991, « Hakim Bey »[244] va signer un ouvrage, la TAZ. En quelques mois, cet essai va être considéré comme le livre théorique qui manquait à l'underground[245].

Hakim Bey, par ailleurs universitaire, évoque le « réseau d'information à l'échelle du globe » créé par les pirates des mers du XVIIIe siècle. *« Il était parsemé d'îles et de caches éloignées où les bateaux pouvaient s'approvisionner en eau et nourriture, et échanger le butin contre des produits de luxe ou de nécessité. Certaines de ces îles hébergeaient des communautés intentionnelles, des micro-sociétés vivant sciemment hors la loi et déterminées à le rester, même si ce n'était que pour une courte, mais joyeuse, vie »*[246].

Hakim Bey parle de la Taz comme étant *« une insurrection sans engagement direct contre l'Etat, une opération de guérilla qui libère une zone (de terrain, de temps, d'imagination), puis se dissout, avant que l'Etat ne l'écrase, pour se réformer ailleurs dans le temps ou l'espace »*[247].

En tant que cyberpunk, il considère le réseau Internet comme le « support logistique » de la TAZ.

Et voici les hackers, comme les pirates des mers trois siècles plus tôt, occupés à créer des TAZ à l'intérieur même du réseau, cherchant ainsi à se réserver des zones d'autonomie, de liberté sur le réseau, en marge de l'Internet étatique et marchand.

Le texte d'Hakim Bey aura donc une double incidence : d'un côté, il incitera les hackers à engager des actions à caractère politique ; et de l'autre, il attirera l'attention de groupes anarchistes « classiques » sur les méthodes du hacking[248].

A côté de la TAZ, un autre élément va également alimenter l'idéologie des hackers : « l'underground ».

---

[244] Son véritable nom est Peter Lamborn Wilson.
[245] Nous reviendrons plus tard sur ce que représente l'underground.
[246] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, p. 44.
[247] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, p. 44.
[248] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 42 à 45.

2) L'Underground

Le concept d' « underground » informatique est apparu avec le Chaos Computer Club de Hambourg (CCC), qui désirait pousser ses réflexions sur les hackers et le phreaking. S'étendant à d'autres sujets (toujours relatifs au haking), l'underground va ainsi désigner, non pas un journal ou un groupe précis, mais un ensemble de relations, d'histoires, d'informations, se répétant à travers le temps et des discussions. L'underground forme un monde à part, avec ses propres règles, imprégnées de l'esprit du hack, comme celle qui veut qu'il ne faut jamais effacer de données sur un système d'informations excepté pour couvrir sa trace[249].

Tout comme l'idéologie, l'esprit du hack ou la TAZ, l'underground va permettre à la communauté des hackers de se structurer, la dotant désormais d'une histoire qui lui est propre.

Pour assurer la continuité du mouvement et la pérennité de la communauté, un contact fort devra toujours être établi entre les anciens et les nouveaux hackers, les Elites formant ainsi les Wannabees et autres Curious Joe.

L'une des questions que nous nous sommes posés était de savoir si l'underground pouvait se voir attribuer une nationalité. Il nous semble que cette distinction ne devrait pas être de mise. En effet, l'undergound étant, par définition, constitué d'histoires, de codes, de « légendes » sur le hack, sur la manière de l'envisager,… celui-ci ne peut qu'être commun à l'ensemble des hackers de la planète.

De même, le fait de se démarquer des autres pays n'a pas réellement de sens pour les hackers, l'esprit du hack et les règles qu'il sous-tend étant communs à l'ensemble des hackers et respectés par tous ceux se présentant comme tels.

Dès lors, ce que certains hackers désignent par underground français, américain,... est plutôt une sorte de galerie de portraits de hackers célèbres dans leurs pays, ce qui est assez paradoxal quand on pense au concept global, mondial, sans frontières représenté par Internet.

Nous pensons qu'il faut plutôt voir dans la « nationalisation » de l'underground un désir de reconnaissance, inhérent à l'activité de hacker, plutôt qu'une volonté de se démarquer réellement d'une histoire dont la base est commune à tous.

Il n'en reste que le concept de « Scène », qui, rappelons-le, peut être considéré comme l'ensemble des hackers, confirmés ou novices, est lui «nationalisable ». Nous trouverons ainsi, par exemple, une Scène américaine avec Kevin Mitnick et Richard Stallman, et une Scène belge avec Asmodeus et RedAttack[250].

---

[249] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 52 et suiv.

[250] Pour rappel, RedAttack est un hacker/cracker (?) belge ayant piraté les sites de plusieurs banques afin de les aider à déceler les failles de leurs systèmes. Sa bonne foi n'ayant pas été prouvée, il fut condamné.

C. HACKERS ET MÉDIAS

Les hackers sont bien conscients de l'importance des médias pour leurs actions et pour l'image que ceux-ci vont donner d'eux.

Comme nous l'avons dit à plusieurs reprises, la plupart des médias ne voient dans les hackers que des cybercriminels de génie, occultant ainsi complètement ce qui constitue la majorité des hackers.

Selon Halbert, les médias jouent un rôle important dans la construction négative de la représentation sociale des hackers. Les médias utilisent les termes « pirates informatiques », « terroristes informatiques » et « hackers » comme synonymes pour parler des activités d'intrusion et des dangers que représentent les pirates informatiques[251].

Or, comme nous l'avons déjà vu, les hackers « purs » légitiment leurs activités par une idéologie particulière, par le « hacking spirit », dont la base est la libre circulation de l'information, ainsi que la gratuité et l'échange réciproque d'informations.

A contrario, les médias peuvent également donner une image tronquée des hackers, en valorisant l'ingéniosité de leur piratage par exemple.

Nous craignons que cette médiatisation excessive du « côté obscur »[252] du hacking ne transforme ce qui n'est au départ qu'une simple fascination, en une volonté de faire pareil, de faire comme les « grands » (hackers).

Prenons un exemple. En 1994, Mark Abene, alias « Phiber Optik », un des leaders des Masters of Deception, est emprisonné pour avoir détourné des lignes téléphoniques. A sa libération, il sera nommé par le « New York Magazine » dans le Top 100 des personnalités les plus intelligentes de la ville.

Cette nomination est un bon exemple de la fascination que les hackers exercent sur les médias. On imagine mal un « simple » braqueur de banque recevoir un titre du même ordre.

Le fait que « Phiber Optik » ait été considéré comme l'une des personnes les plus intelligentes est certainement pertinent, mais cette manière de faire nous semble de nature à banaliser, voire encourager, les actions de piratage informatique. Cela n'aurait peut-être pas été le cas si cela avait été le fait d'un magazine spécialisé dans la cyberculture, mais c'était ici un magazine généraliste, et n'ayant donc pas de connaissances aussi poussées en la matière.

Le risque de voir les pirates informatiques devenir des héros aux yeux des jeunes hackers ne nous semble pas à négliger, comme l'ont d'ailleurs compris les hackers « old school » et autres participants des congrès DefCon, soucieux de valoriser, cette fois, le « bon côté de la force ».

---

[251] D., HALBERT, « Discourses of Danger and The Computer Hacker », The Information Society, 1997, n°13, pp. 361 à 374.

[252] Ce terme fait référence au film « Star Wars », qui est très apprécié par les hackers, comme d'ailleurs tout ce qui touche à la science-fiction et à la cyberculture, comme nous l'avons vu.

Ceux-ci ont à plusieurs reprises voulu démontrer qu'ils étaient autre chose que des délinquants. Dans cette optique, ils ont publié sur les Net des dizaines de textes, d'essais, sur ce qu'est véritablement un hacker.

Ces textes donnent l'occasion d'obtenir des informations issues du sein-même de la communauté des hackers, et ainsi d'en savoir plus sur leurs volontés, leurs sentiments, leurs aspirations.

Parmi tous ces textes, nous en avons retenu deux parmi les plus célèbres, le «Manifeste du Hacker »[253] et « The Hacktivismo Declaration »[254] que nous reproduisons en annexe.

Les hackers se plaignent souvent que la majorité des personnes peu familières des réseaux informatiques méconnaissent totalement la nature des rapports sociaux qui peuvent y être créés et entretenus.

Pour Jordan et Taylor[255], ceci explique que les hackers sont souvent dépeints comme des criminels, vivant la nuit, environnés de secrets et réalisant des exploits impossibles. Cette peur instinctive doit être mise de côté si l'on désire appréhender correctement le monde des hackers.

C'est ce que nous explique « The Mentor », exprimant dans son « Manifeste du hacker » le sentiment d'incompréhension ressenti par de nombreux hackers.

Dans le second texte, « The Hacktivismo Declaration », rédigé en accord avec l'esprit du hack, les hackers décrivent leur ligne de conduite. Véritable « déclaration d'indépendance des hackers »[256], ce texte promeut la liberté de dire et de penser, quel qu'en soit le prix (au sens moral), ainsi que la capacité à lutter pour que chacun puisse exprimer ses idées librement, en ce compris celles qui vont à l'encontre des idées défendues par les hackers.

Le but des auteurs de ce texte est donc, d'une part, de revendiquer la liberté d'expression et de réaffirmer leur volonté de se battre jusqu'au bout pour la conserver (tout en étant d'accord de la restreindre dans certains domaines comme la pédo-pornographie, certains secrets d'Etats, relatifs à la vie privée,…), et d'autre part, de montrer que ces revendications sont faites en vue du bien commun de tous, et non exclusivement des hackers.

Ils perpétuent ainsi l'esprit du hack originel, prônant la liberté, le progrès et le bien-être de l'Humanité.

---

[253] THE MENTOR, « Le manifeste du hacker », http://biblioweb.samizdat.net/, 8 janvier 1986. Ce texte est reproduit en annexe.

[254] HACKTIVISMO, CULT OF THE DEAD COW, « The Hacktivismo Declaration », www.cultdeadcow.com, 4 juillet 2000. Ce texte est reproduit en annexe.

[255] T., JORDAN, P., TAYLOR, « A sociology of hackers », Sociological Review, nov. 46(4), 1998, pp. 757 à 780.

[256] C'est d'ailleurs l'autre nom sous lequel est connu ce texte.

D. LES HACKERS ET L'ÉTHIQUE

Basiquement, l'éthique est par définition la *science de la morale*, elle-même *science du Bien et du Mal*. La question de la définition des notions de bien et de mal est donc le fondement de toute éthique[257].

Les différents éléments qui viennent d'être développés démontrent bien qu'il y a une réelle volonté des hackers à se créer une histoire, des règles, et partant, à distinguer les «bons » hackers des « mauvais ».

Comme nous l'avons vu, les hackers n'ont pas, la plupart du temps, l'impression que leurs intrusions peuvent être néfastes.

Prenons une famille «classique ». Les parents éduquent leurs enfants, leur disant ce qui est bien et ce qui ne l'est pas. Les enfants savent ainsi qu'ils ne doivent pas voler, ni se droguer par exemple.

Par contre, peu de parents interdisent à leurs enfants de pénétrer les ordinateurs du Pentagone (l'exemple est ici volontairement caricatural, même si le Pentagone, comme nombres d'institutions étatiques, est une des cibles privilégiées des hackers).

De même, l'intrusion informatique n'a pas la même connotation négative qu'un cambriolage par exemple, et ce, tout simplement parce que les gens « étrangers » au hacking, n'ayant pas les connaissances suffisantes que pour appréhender ce domaine, n'en mesurent pas nécessairement les conséquences. Si tout le monde sait ce qu'est un cambriolage, beaucoup moins savent ce qu'est un cheval de Troie et l'usage qui peut en être fait.

Dès lors, le sens moral du hacker ne se développe souvent qu'au contact de ses «pairs », des autres hackers au sein de la communauté. Cette communauté se forge une idéologie, des valeurs communes (l'esprit du hack), une histoire (l'underground), un univers qui lui est propre (la TAZ),… de sorte qu'elle n'est pas à proprement parler régulée de l'extérieur. Si elle devait se soumettre à la loi, c'est à contre-cœur, par obligation. Les hackers forment un monde à part, érigeant eux-mêmes leurs codes, leurs lois, leurs sanctions et leur vision personnelle du Bien et du Mal.

Cette assimilation à un groupe et l'acceptation de ses normes sont des concepts qui ont notamment été développés par Sutherland.

---

[257] S., GHERNAOUTI-HELIE, *Sécurité Internet, Stratégies et technologies*, Paris, Dunod, 2000, pp. 38 et suiv.

1) La théorie des associations différentielles de Sutherland

Ce schéma rentre dans la théorie des associations différentielles développée par Sutherland[258]. Il y explique que le comportement délinquant est un comportement appris au contact d'autres personnes par un processus de communication. Ces personnes sont des relations personnelles, des membres du groupe, de la bande.

La théorie de Sutherland exclut l'influence des médias. C'est un point important à mettre en rapport avec l'esprit du hack. En effet, l'idéologie des hackers repose notamment sur le fait que ce ne sont pas les médias qui font de vous un hacker, mais bien la reconnaissance des autres hackers, et seulement eux[259]. Il est clair que certaines personnes peuvent avoir envie de se lancer dans une carrière de hacker en voyant les exploits de certains relatés par les médias, mais cette volonté ne fait pas de vous un hacker. Il vous faudra faire vos preuves, montrer votre appartenance au groupe, à ses règles (le secret, l'anonymat,…)[260], aux mobiles de ses actions[261].

Ce dernier point est également à mettre en parallèle avec la théorie de Sutherland, tout comme le fait que les délinquants utilisent des causes de justification de leurs actes, qui, dans le cas des hackers, seront principalement la défense des libertés et le progrès de l'Humanité.

Enfin, la base de la théorie de Sutherland est le principe des associations différentielles, qui veut que l'individu ne devienne délinquant que lorsque les interprétations défavorables au respect de la loi l'emportent sur les interprétations favorables.

C'est clairement le cas des hackers, qui dans la majorité des cas, se retrouvent en contradiction avec la loi, qu'ils ne voient généralement que comme un frein à leurs libertés (d'expression, d'information…). A contrario, les normes établies par la communauté (des pirates) seront considérées favorablement par les hackers, car elles sont les seules à même de leurs assurer ces libertés[262]. Les délinquants informatiques respectent les mêmes valeurs que les gens «normaux », mais pas de la même manière. Ils correspondent ainsi à «l'innovateur » décrit par Merton, comme nous le verrons plus tard.

---

[258] E., SUTHERLAND, D., CRESSEY, *Principes de criminologies*, Paris, Cujas, 1996, pp. 89 et suiv.
[259] Cf. supra.
[260] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 81 et suiv.
[261] Pour rappel, il s'agit là d'un point-clé de l'idéologie des hackers.
[262] Nous ne visons pas ici les cybercriminels, les crackers, qui eux, comme nous l'avons dit, n'adhèrent pas à l'esprit du hack, ni à l'idéologie qui en découle.

2) La notion du Bien et du Mal chez les hackers

Revenons à l'éthique des hackers. La question du « bien et du mal » dans le cas des hackers est similaire à la question de savoir s'il est bien ou mal de voler lorsqu'on a faim. Cette question n'a pas vraiment de sens. Tout comme (dans ce cas précis) on ne vole pas pour faire du mal mais bien pour manger, les hackers ne s'introduisent généralement dans les systèmes que pour assouvir leur passion, leur intérêt presque scientifique pour l'informatique, sans réellement catégoriser leur action.

Cette dernière remarque ne s'applique évidemment pas aux crackers et autres Blacks Hats, qui sont eux parfaitement conscients de la teneur réelle de leurs actes.

Nous ne cherchons pas ici à défendre les hackers, mais bien à démontrer que leur mode de pensée est différent du délinquant « moyen », pour la simple raison qu'ils n'ont pas l'impression d'être des délinquants.

A titre d'exemple de la difficulté à classer tel ou tel groupe de hackers dans un ou dans l'autre camp, l'affaire du groupe « hacktiviste »[263] « Legions of Underground »[264].

En 1998, les « Legions of Underground »[265] (LoU) commencent par « defacer »[266] un site créé par le gouvernement chinois. Ensuite, en représailles à l'exécution de deux hackers chinois, ils débloquent plusieurs accès à des sites censurés par le même gouvernement, et finissent pas déclarer la guerre électronique totale à la Chine, ainsi qu'à l'Irak en appelant la Scène à la destruction complète de tous les systèmes d'information de ces pays.

Mais, en janvier 1999, la Scène réagit et les groupes en vue tels que le CCC ou encore Hispanahack se désolidarisent du mouvement lancé par les LoU et dénoncent toute tentative qui viserait à détruire l'infrastructure de communication d'un pays. Se posant comme les défenseurs de l'esprit du hack, tout en veillant à protéger leurs intérêts et à ne pas scier la branche sur laquelle ils sont assis, ces groupes s'engagent à *« laisser les réseaux de communications intacts »* considérant ceux-ci comme les centres nerveux de notre planète.

Les LoU sont ainsi mis au ban de la « société du hack », non sans contradiction d'ailleurs, notamment avec l'Hacktivismo Declaration.

Dès lors, qui sont les « bons » et les « mauvais » hackers ? Les LoU qui revendiquent et défendent la liberté d'expression et l'esprit du hack, en accord complet avec l'Hacktivismo Declaration, texte fondateur de l'esprit du hack, ou les CCC et autres groupes, se revendiquant également de l'esprit du hack, mais qui ont refusé de se lancer dans une guerre électronique, conscients des dégâts qui pourraient être faits et désireux de rester dans les limites de la légalité ?

---

[263] Nous verrons plus tard ce que l'on entend par hacktivisme.
[264] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 61 et suiv.
[265] Ce groupe possède son propre site Internet à l'adresse www.legions.org.
[266] Cf. supra.

Si l'on se place du côté de la loi, la réponse est évidente, mais si l'on se place du côté des hackers, il nous semble qu'elle posera beaucoup plus de problèmes, divisant vrais et faux naïfs : ceux qui suivent aveuglément l'esprit du hack et ceux qui en comprennent les limites…

3) La théorie des conflits de culture de Sellin

La théorie de Sutherland, son application aux hackers, ainsi que leur conception du Bien et du Mal, peuvent être rapprochées de celle des « conflits de culture » développée par Sellin[267].

Sellin considère le comportement délinquant comme un comportement conforme à des normes qui sont en conflit avec les normes de la société. La délinquance sera alors l'expression de ce conflit de culture. C'est le cas pour les hackers qui, comme nous venons de le dire, adoptent les normes en vigueur dans le groupe, normes qu'ils considèrent comme tout à fait normales.

Pour Sellin, il faut relativiser les notions de Bien et du Mal, celles du conformisme et du non conformisme, car tout dépendra de l'appartenance de l'individu à tel ou tel groupe.

Ici aussi, l'application aux hackers est pertinente, ceux-ci ayant leur propre vision du Bien et du Mal, fonction de la vision du groupe, de ses objectifs et de ses normes[268].

Enfin, Sellin met l'accent sur la définition du comportement et sur le comportement même, si bien que c'est selon cette définition que le comportement sera considéré comme conforme ou non.

Cette théorie s'applique également aux hackers, en particuliers aux hackers « purs », qui ne voient pas leurs actes comme des actes néfastes, mais au contraire, comme des actions utiles à la société. Ils ont ainsi une autre définition, une compréhension de leur comportement que celle adoptée par la société en général.

---

[267] T., SELLIN, *Culture Conflict and Crime*, New York, Social Science Research Concil, 1938, pp. 58 et suiv.
[268] Cf. supra.

Section 3 – Profils et motivations du hacker

Les nombreux paradoxes du hacker viennent d'être révélés dans la partie qui précède :

- Le hacker a le droit de s'introduire partout, mais n'accepte pas que l'on s'introduise chez lui.
- Il ne supporte pas que l'on viole sa liberté d'expression, mais se permet quant à lui de juger et de « sanctionner » ce qui lui plaît et ne lui plaît pas
- Enfin, et c'est peut-être le plus évident, il s'introduit discrètement, sans laisser de traces, mais une fois son forfait accompli, signe son action.

Pour comprendre cette logique, il faudrait presque être un hacker soi-même, ou du moins avoir une véritable connaissance de tout ce qui les concerne.

Et c'est peut-être bien là que réside le problème lorsqu'il s'agit de parler des hackers. Aucun néophyte ne peut comprendre leurs actions, leurs schémas de pensée au travers de leurs simples intrusions médiatiques.

Ce manque de connaissances réelles, issues de l'underground ou de la communauté-même, est la raison pour laquelle de nombreux experts, auteurs, se sont trompés dans leur description du hacker.

Dans cette partie, nous aborderons d'abord les facteurs criminogènes relatifs à la criminalité informatiques. Ceux-ci soulignent quelques éléments «objectifs » permettant d'expliquer, en partie, l'importance des dégâts causés par la criminalité informatique et la relative impunité de ses auteurs[269].

Ensuite, nous nous poserons la question de savoir si un profil-type du criminel informatique peut être établi.

Enfin, nous terminerons par un passage en revue des différentes motivations des hackers, qui permettront de comprendre que la criminalité informatique poursuit des buts aussi variés que la revendication politique, le défi intellectuel, le profit personnel ou encore l'emploi.

Nous conclurons cette partie en insistant sur la relation existant entre la motivation au passage à l'acte et la théorie du choix rationnel et celles des opportunités, ainsi que, succinctement, la typologie de Merton, pour terminer par déterminer l'utilité de la connaissance des motivations des hackers pour les autorités policières.

.

[269] Il est à noter que ce dernier point a déjà été abordé, notamment dans la partie consacrée aux similitudes existant entre criminalité informatique et criminalité en col blanc.

A. FACTEURS CRIMINOGÈNES

Une série de facteurs criminogènes sont caractéristiques de la criminalité informatique[270] :

① Il y a tout d'abord le niveau d'intelligence, d'ingéniosité des pirates informatiques. Il est clair que s'introduire sur un ordinateur n'est pas dans les possibilités de n'importe qui, le simple deface de site nécessitant quand même un minimum de connaissance, contrairement au meurtre ou au vol à la tire par exemple.

② Les entreprises sont souvent pressées d'entamer leurs activités, et ce, parfois au détriment des mesures de sécurité, alors que, comme nous l'avons vu dans la partie consacrée aux risques, la question des moyens de sécurité est déterminante en matière de criminalité informatique. Ce point est un des éléments expliquant la relative impunité des pirates informatiques.

③ L'infaillibilité de l'ordinateur. Ou plutôt le fait que son utilisateur le croit infaillible. Pour l'anecdote, il est amusant de constater que cette infaillibilité devient relative devant un client mécontent (*« c'est pas moi, c'est l'ordinateur qui… »*).

④ Le faible risque de voir la fraude découverte. En effet, les criminels peuvent facilement supprimer la preuve de leurs méfaits en effaçant simplement les données. De plus, les avocats, les juges ne sont pas toujours à même de saisir toutes les subtilités de l'informatique[271].

⑤ N'étant pas un crime de sang et ne plaçant pas (toujours) la victime en présence directe de l'auteur de l'infraction, la délinquance informatique peut prendre l'aspect d'un jeu, d'un défi entre deux cerveaux. La notion de défi, de jeu, de curiosité est une des motivations régulièrement avancées par les hackers pour expliquer leur crime, comme nous le verrons dans un instant.

Si des facteurs criminogènes peuvent être pointés, un profil-type peut-il pour autant être établi ?

---

[270] X, « Fraude informatique : danger ! - Rapport du Comité européen des problèmes criminels », Data News, n°19 du 4 oct. 1983, pp. 14 et s.

[271] U., SIEBER, *La délinquance informatique*, Bruxelles, Story scientia, Précis et travaux de la Faculté de droit de Namur, n°9, 1990, pp. 196 et suiv.

B. LE PROFIL-TYPE DU CRIMINEL INFORMATIQUE EXISTE-T-IL ?

Avant toute chose, il nous faut préciser que nous envisageons le profil type dans son « acception policière », permettant aux autorités de trouver plus facilement les cybercriminels. Nous ne viserons donc pas ici les motivations des hackers (qui seront abordées plus loin), mais bien l'existence ou non d'une série de caractéristiques intrinsèques aux hackers.

La question de l'existence et/ou de la pertinence du profil type nous semble particulièrement importante en matière de criminalité informatique.

Nous sommes bien conscients que la criminalité informatique est fortement marquée par l'influence du chiffre noir, la délinquance apparente n'étant pas représentative de la criminalité réelle ; mais il nous semblait intéressant de voir si d'autres obstacles existaient à l'établissement d'un profil type du hacker.

Les victimes ne pouvant généralement pas donner de détails concernant les malfaiteurs, ceux-ci opérant le plus souvent à distance, la découverte de caractéristiques intrinsèques aux hackers devrait permettre aux autorités de les appréhender plus facilement.

Comme nous l'avons vu précédemment, les hackers présentent autant de diversités que les crimes qu'ils commettent. Ils attaqueront ainsi tantôt en bande, tantôt en solitaire, tantôt avec des intentions bienveillantes, tantôt dans le but de nuire,…. Si bien que l'établissement d'un profil type ne sera pas d'un grand secours dans le cadre d'une recherche policière. Ainsi, à titre d'exemple :

- Y a-t-il une tranche d'âge déterminée ? Non, les plus anciens hackers ayant dépassé les 60 ans[272] ;
- Sont-ils d'une nationalité déterminée, ont-ils des convictions religieuses spécifiques ? Cette question est vidée de son sens par l'idéologie même des hackers[273] et l'aspect transfrontalier du réseau Internet[274]. Les hackers sont partout, de toutes nationalités et de toutes religions ;
- Occupent-ils des emplois spécifiques ? La réponse est également non. On trouve des étudiants comme des employés de banque ou encore des personnes occupant des professions littéraires[275].
- …

D'ailleurs, Chris Goggan, membre des LoD[276], ne déclarait-il pas lui-même que parmi les hackers *« on trouve tous les niveaux de revenus, toutes les races, toutes les religions »* ?[277].

---

[272] Cf . supra.
[273] Cf. supra.
[274] Cf. supra.
[275] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, p. 145.
[276] Cf. supra.

Dès lors, à l'exception d'une passion pour l'informatique et les nouvelles technologies[278], les hackers ne présentent pas de caractéristiques intrinsèques permettant d'établir un profil-type. Il nous paraît donc que cette seule caractéristique commune à tous les hackers ne constituera pas une aide très précieuse pour la police. Nous verrons d'ailleurs plus tard que la Computer Crime Unit (la section de la police belge chargée des crimes informatiques), n'utilise pas de profil-type et travaille uniquement sur plainte, la somme de travail étant déjà trop importante que pour avoir recours à la proactivité.

---

[277] C., GOGGANS, « Hackers aren' the real enemy », Computerworld, 8 juin 1992.

[278] Nous parlons bien ici de passion et non de capacités, de connaissances, tous les hackers (au sens large) n'étant pas des virtuoses de l'informatique (cf. les script-kiddies abordés supra).

C. LES MOTIVATIONS DES HACKERS

Tout comme la criminalité informatique, les motivations des cybercriminels sont multiformes.

Certains auteurs considèrent que l'on peut cerner cinq groupes de motivations (sociale, technique, politique, financière et étatique)[279], d'autres définissent des catégories de délinquants en fonction de leurs motivations.

Parmi ceux-ci, nous avons décidé d'aborder la typologie réalisée par Donn Parker[280].

1) La typologie de Donn Parker

La typologie de Donn Parker nous paraît être l'exemple à ne pas suivre, tant les catégories qu'il définit nous semble constituer des catégories « fourre-tout », vidant par là même l'utilité d'une catégorisation. Parker définit sept catégories de délinquants informatiques[281] : les amateurs, les détraqués, le crime organisé, les gouvernements étrangers, les criminels professionnels, les extrémistes idéalistes et les casseurs systèmes. Par souci de concision, nous ne détaillerons que les trois premières catégories, celles-ci étant suffisamment caractéristiques de la typologie établie par Parker ainsi que de ses défauts, le but étant de démontrer que ces catégories ne sont pas pertinentes sur le plan des motivations.

- Les **amateurs** : il s'agit, pour Parker, de « gens ordinaires », qui détiennent des postes clés ou ayant des connaissances informatiques. Leurs problèmes sont d'ordre personnel, comme par exemple l'argent, la famille ; liés à l'alcool ou au jeu ; ou encore d'ordre professionnel. La motivation de leurs délits est la résolution de ces problèmes.

Pour notre part, outre le fait que nous considérons étonnant de mettre sur un même pied des motivations comme le jeu et la vengeance, nous ne voyons pas en quoi le crime informatique peut résoudre un problème lié à l'alcool par exemple.

- Les **détraqués** : Parker vise ici le «programmeur fou » qui saccage les ordinateurs de la salle informatique où il travaille.

Deux éléments nous interpellent. D'une part, bien que Parker considère qu'il s'agit de faits tout à fait exceptionnels, il en fait malgré tout une catégorie à part entière. D'autre part, le simple fait de détruire du matériel informatique ne fait pas de vous un criminel informatique ! Il suffit de s'en référer aux différentes définitions[282] de la criminalité informatique pour s'en convaincre.

---

[279] S., GHERNAOUTI-HELIE, *Sécurité Internet, Stratégies et technologies*, Paris, Dunod, 2000, pp. 37 et suiv.
[280] D.-B., PARKER, *Combattre la criminalité informatique*, Paris, Oros, 1985,
[281] Nous tenons à préciser que les définitions qui sont paraphrasées ici sont établies par Donn Parker lui-même, et que nous n'adhérons pas nécessairement à celles-ci.
[282] Cf. supra.

- Le **crime organisé** : Selon Parker, la mafia (qu'il considère comme étant le crime organisé au sens strict du terme) peut voir dans le crime informatique un moyen de diversifier ses activités traditionnelles que sont la drogue, le jeu, la prostitution et le racket.

Si l'on suit le raisonnement de Parker, le crime organisé constitue une catégorie de criminels informatiques. Nous considérons ceci comme peu pertinent, ne serait-ce que parce que le crime organisé, comme le dit Parker, poursuit des activités qui ne nécessitent pas toutes l'intervention de l'informatique (que ce soit comme but ou comme moyen de commettre l'infraction), alors que, comme nous l'avons vu, Parker définit lui-même le crime informatique comme *« tout acte illicite nécessitant une connaissance spécialisée de l'informatique, au stade de la perpétration, de l'enquête de police ou des poursuites pénales »*[283].

En réalité, Donn Parker ne réalise pas une classification des cybercriminels selon leurs motivations, mais plutôt selon la «nature » des criminels. Le fait d'être un amateur ou un détraqué ne constituant pas une motivation, mais tenant plutôt du profil-type, Parker démontre ainsi, sans le vouloir, qu'une fois de plus la pertinence d'un profil-type en matière de criminalité informatique n'est pas avérée.

En effet, si l'on regroupe toutes ces catégories, nous n'obtenons pas l'ensemble des criminels informatiques[284], mais bien l'ensemble de la population, puisque s'y retrouvent les amateurs (au sens entendu par Parker), les détraqués et les criminels professionnels, voire même les gouvernements, si bien que nous nous posons la question de savoir qui ne rentre pas dans une de ces catégories.

Comme nous venons de le voir, le fait de chercher nécessairement à regrouper l'ensemble des motivations en catégories nous semble être une source d'erreur. Il apparaît en effet, comme en ce qui concerne les différentes formes que peut prendre la criminalité informatique[285], que les motivations des hackers sont trop diverses que pour pouvoir constituer des groupes parfaitement homogènes.

Dès lors, il nous semble plus pertinent de n'envisager que ce que nous considérons comme les « principales » catégories de motivations, étant entendu que celles-ci ne sont pas exhaustives et que d'autres motivations peuvent exister, en marge de ces catégories.

---

[283] D.-B., PARKER, *Combattre la criminalité informatique*, Paris, Oros, 1985, p.18

[284] Nous ne rentrons pas ici dans les considérations relatives à la criminalité réelle et la criminalité constatée.

[285] Nous verrons plus tard que catégoriser les différentes formes de criminalité pose également certains problèmes.

2) Les principales motivations des hackers

D'une manière générale, le crime informatique est rarement commis de manière impulsive (à l'exception de quelques cas de sabotage). Il est généralement le fruit d'une période de réflexion, durant laquelle le cybercriminel met en balance les intérêts qu'il peut retirer de son infraction et les risques qu'elle représente[286]. Nous y reviendrons.

Selon Cusson[287], les criminels justifient généralement leurs actes avec plusieurs arguments : la vengeance, la peine «rétributive » (la victime n'a que ce qu'elle mérite), le mérite ou le courage et enfin la négation du dommage.

Ces arguments ont été choisis à dessein car ils constituent souvent des mobiles avancés par les pirates informatiques.

Ainsi, comme nous l'avons vu, parmi les criminels informatiques se trouvent d'anciens employés virés de leur société et désireux de se venger ; des personnes aux revendications libertaires, prêtes à tout pour affirmer leurs idées[288] ; des jeunes en manque de reconnaissance sociale et désireux de vouloir devenir quelqu'un sur la Scène[289] ; et, également, de faux naïfs, niant systématiquement l'importance de dégâts causés[290].

Ces motivations ne sont pas les seules à pouvoir être dégagées. Nous serions tentés de dire qu'il y a autant de motivations différentes qu'il y a de hackers, si bien que nous ne présenterons ici que ce qui nous semble constituer les principales catégories de motivations, qui, répétons-le, ne sont pas exhaustives.

---

[286] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, pp. 215 et suiv.
[287] M., CUSSON, *Le contrôle social du crime*, Paris, PUF, 1983.
[288] Cf. supra.
[289] Cf. supra.
[290] Cf. supra.

a) Les motivations liées à l'argent et au profit en général

La recherche d'un gain financier représente la motivation la plus répandue chez les criminels informatiques (ce qui, comme nous l'avons vu, les rapproche de la criminalité d'affaires).

Les cas ne manquent pas, et sont généralement les plus médiatisés, que ce soit aux Etats-Unis ou en Europe[291]. Le dénominateur commun à tous ces cas est généralement la découverte d'une faille dans un système informatique[292] qui sera utilisée pour s'approprier un profit financier direct (par exemple dans le cas du détournement de fonds) ou indirect (par exemple dans le cas du détournement d'informations ou de l'espionnage économique)[293].

Le gain financier comme motivation du crime informatique répond aux principes de la théorie économique : il s'agira, pour le pirate informatique, de maximiser ses gains et de minimiser ses contraintes et ses risques[294].

Le recours à l'informatique est dès lors particulièrement judicieux car il permet, avec un minimum d'investissement (personnel et financier) d'obtenir des gains très importants.

Enfin, il nous paraît utile de préciser que le gain financier peut prendre plusieurs formes, comme par exemple l'emploi.

Ainsi, si la cybercriminalité est avant tout une menace, elle n'en reste pas moins une opportunité pour certains pirates de se faire connaître sur le marché de l'emploi.

Ce fut par exemple le cas du créateur du virus Kournikova – l'un des virus ayant causé le plus de dégâts ces dernières années[295] - qui s'est vu proposer du travail, quelques heures seulement après son arrestation.

De même, des sociétés éditrices de jeux, opportunistes, lancent parfois des appels directement à partir de leurs logiciels. C'était ainsi par exemple le cas de la société Cobra soft (qui n'existe plus aujourd'hui)[296].

Mieux, Petar Stoïanov, président de la République de Bulgarie, a déclaré être prêt à embaucher « Kubaka », le hacker ayant détourné le site officiel de la présidence le 16 janvier 2001 afin de protester contre la misère et le chômage des jeunes : *« Il a piraté le site avec habileté, aussi, s'il se présente, je n'hésiterais pas à le prendre pour travailler avec moi »*[297].

---

[291] Voy. S., LE DORAN, P., ROSE, *Cyber-thrillers, 35 histoires vraies de délinquance informatique*, Paris, Albin Michel, 1996.
[292] Nous y reviendrons plus loin.
[293] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, pp. 216 et suiv.
[294] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, pp. 216 et suiv.
[295] De nombreuses informations peuvent être trouvées concernant ce virus, et les virus en général, sur le site de Norton (l'un des principaux éditeurs d'anti-virus) www.norton.com.
[296] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 33 et suiv.
[297] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 33 et suiv.

Le fait de décrire l'emploi comme une motivation pouvant amener un hacker à exercer une activité criminelle n'était peut-être qu'une boutade, mais traduit néanmoins une tendance actuelle très nette.

Olivier Bogaert, inspecteur principal à la CCU, nous a ainsi confirmé que certains pirates envoyaient des e-mails à leurs « futures » victimes, dans lesquels ils disaient avoir trouvé les failles du système informatique et proposaient, moyennant paiement, de les aider à sécuriser celui-ci (quand ce ne sont pas les victimes elles-mêmes qui contactent les pirates afin qu'ils changent de camps et protègent ce qu'ils ont précédemment attaqué).

Même si ce dernier exemple tient beaucoup plus du chantage que de la lettre de motivation classique, ce type d'approche est néanmoins souvent couronné de succès pour le hacker. A moins que ce ne soit sa victime la réelle gagnante de ce jeu de dupe ?

b) Les motivations d'ordre intellectuel : le jeu et le défi

Le jeu constitue la motivation la plus connue, parce qu'il apparaît généralement dans les cas médiatisés de pénétration de systèmes ou de piratage de logiciels[298]. Les membres du Chaos Computer Club expliquent ainsi que *« le pirate moyen a des motivations moyennes : le goût du jeu, de l'aventure, le sentiment de puissance face à un instrument sophistiqué (appartenir à l'élite secrète !) et, en filigrane, le rêve du grand coup. Au nom de ces mobiles, on fait tout ce qui est faisable. Sans avoir clairement conscience de commettre un acte répréhensible »*[299].

Bien souvent, la différence entre le jeu et la recherche de profit est difficile à établir, si bien qu'on considère souvent que ces motivations sont toutes les deux présentes.

Il n'en reste que l'aspect « jeu » ou « défi intellectuel » est présent dans la majorité des crimes informatiques, ce qui s'explique par plusieurs raisons.

Tout d'abord, le hacker va trouver dans le jeu la reconnaissance sociale qui caractérise les hackers les plus doués. En effet, depuis l'antiquité, le jeu (et, par extension, le combat, en référence aux jeux du cirque), a toujours été synonyme de valeur, de courage et de volonté d'être[300].

Ensuite, il faut une certaine dose d'incertitude : *« le jeu ne divertit plus celui qui, trop entraîné ou trop habile, gagne sans effort et infailliblement (…). Il faut un renouvellement constant et imprévisible de la situation (...). Le jeu consiste dans la nécessité de trouver, d'inventer immédiatement une réponse qui est libre dans les limites des règles. Cette latitude du joueur (...) explique en partie le plaisir qu'il suscite »*[301].

La contrainte joue également un rôle paradoxal. Si elle est librement acceptée dans le cadre du jeu, ce n'est pas le cas dans celui du travail. On le voit par exemple avec les hackers, qui bien souvent très intelligents, se trouvent en situation d'échecs scolaires, les contraintes éducatives leur étant insupportables, contrairement à celles liées au piratage[302]. Il faut en effet se plier aux « règles » de pénétration d'un système informatique, à commencer par la contrainte de trouver un mot de passe valable. Et si ces contraintes sont acceptées, c'est parce qu'elles font appel à l'imagination et aux facultés d'adaptation du pirate, lui permettant ainsi de prouver toute son ingéniosité.

Enfin, une série de caractéristiques propres au joueur sont transposables aux criminels informatiques. Ce qui intéresse le joueur, et - serions-nous tentés de dire consécutivement aux différents éléments déjà développés - le hacker, c'est *« avant tout le défi, la compétition où il peut se révéler un gagneur. Les lents et les prudents l'impatientent. Il aime prendre des risques et pousser les autres au-delà de leur allure normale. Il réagit au travail et à la vie comme à un jeu. La lutte le galvanise (…). Son principal but (…) c'est d'être un gagnant, et à chaque fois*

---

[298] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, p.217.
[299] CHAOS COMPUTER CLUB, *Danger pirates informatiques*, Paris, Plon, 1989, p. 109.
[300] A., LWOFF, « Le jeu et l'idée dans la création scientifique », Science et Avenir, mai 1976, pp. 506 à 510.
[301] R., CAILLOIS, *Les jeux et les hommes*, Gallimard, 1967, pp. 38 à 39.
[302] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, p.218.

qu'on parle de lui, on aboutit invariablement à une discussion sur sa tactique et sa stratégie dans les luttes de l'entreprise (…). Il aime prendre des risques calculés ; la technique et les méthodes nouvelles le fascinent (…). Il est coopératif, mais compétitif ; désinvolte et enjoué, mais irrésistiblement attiré par la réussite ; c'est un bon coéquipier, mais il aspire au vedettariat, (…) mais aussi un rebelle contre la hiérarchie bureaucratique (…). Son but principal est d'être connu comme un gagnant ; sa crainte la plus profonde, d'être étiqueté comme un perdant (…). Quand ils laissent retomber leur excitation. Ils se trouvent confrontés au sentiment d'impuissance. Les plus motivés des joueurs ont besoin d'être branchés, électrisés sous le courant de la compétition. Privés de défis au travail, ils s'ennuient et deviennent légèrement dépressifs »[303].

On ne peut manquer d'être frappé par la correspondance entre ces divers éléments et les valeurs de référence de la majorité des hackers.[304]

Un élément essentiel est à pointer en ce qui concerne la notion de jeu chez les hackers, à savoir le fait que ceux-ci déclarent se référer à une déontologie[305].

A ce titre, le Chaos Computer Club déclare que les hackers respectent les principes suivants : *« un pirate, ce n'est pas quelqu'un qui, doué d'une énergie criminelle, ou par pur vandalisme, commet des dégâts ; c'est quelqu'un qui se penche de manière critique sur les choses qui ont éveillé son intérêt. Un système de sécurité, le plus sophistiqué soit-il, perd, avec le temps qui passe, la moitié de son efficacité. Il y aura toujours que/qu'un pour trouver la faille. L'homme est imparfait. Pirater, c'est une aventure, mais cela n'est pas un but en soi. Cela permet simplement de comprendre comment ça marche »*[306].

Il y aurait donc une sorte d'autodiscipline des hackers, qui explique également leur aversion vis-à-vis de ceux qui détruisent ou affectent les données « visitées », comme les crackers et les crashers[307].

Enfin, le jeu, plus qu'une motivation, peut devenir une source de justification pour les hackers, tentant ainsi d'atténuer la portée de leurs actes. Chris Goggans déclarait ainsi que *« depuis onze ans, j'ai eu la possibilité de devenir riche. Je n'ai pas été tenté. J'ai certes regardé derrière des portes sur lesquelles était inscrit « Accès réservé au personnel autorisé », mais je n'ai jamais empêché le fonctionnement des ordinateurs. Il faut distinguer le voyeurisme du viol. Le problème reste l'administration déficiente de la plupart des systèmes »*[308].

---

[303] M., MACCOBY, Le joueur, Paris, InterEditions, 1980, pp. 19 à 20 et 59 à 67.
[304] Cf. supra.
[305] P., ROSE, J.-M., LAMERE, Menaces sur les autoroutes de l'information, Paris, L'Harmattan, 1996, pp.221 et suiv.
[306] CHAOS COMPUTER CLUB, Danger pirates informatiques, Paris, Plon, 1989, p. 109.
[307] Nous avons vu précédemment que les hackers purs leur reprochaient leur manque de connaissances informatiques et, d'une manière plus générale, de ne pas respecter le hacking spirit.
[308] C., GOGGANS, « Hackers aren' the real enemy », Computerworld, 8 juin 1992.

Avec cette dernière phrase, Goggans fait référence aux motivations premières de tout hacker « pur », à savoir la liberté d'information et le progrès de l'Humanité.

Le fait de vouloir s'introduire dans un système informatique dans un but bienveillant est une justification récurrente chez les hackers, considérant qu'ils ne commettent pas un délit mais cherchent à aider l'Humanité en repoussant les limites de la machine[309].

La question que nous nous sommes posés est de savoir pourquoi les hackers « bienveillants » n'allaient pas directement proposer leurs services aux sociétés considérées comme défaillantes sur le plan de la sécurité, plutôt que s'introduire illicitement sur leur système. Nous pensons que la réponse est à chercher dans le défi intellectuel consistant à pénétrer un système et la reconnaissance auprès des pairs que la réussite de ce défi va engendrer. Celle-ci, couplée au sentiment d'altruisme engendré par le signalement des failles du système auprès des administrateurs permettra, à notre sens, au hacker d'obtenir ainsi une double source de satisfaction : il sera reconnu par ses pairs mais également par la Société, celle-ci ne voyant généralement en lui, au mieux qu'un gamin, au pire qu'un criminel. Ceci n'est évidemment qu'une hypothèse, mais nous l'estimons fondée, au regard de ce qui vient d'être exposé concernant les hackers, leur histoire, leurs valeurs et leur idéologie.

De même, si ces louables intentions sont certainement sincères pour les hackers « purs », nous nous posons la question de savoir si celles-ci ne risquent pas, comme le jeu, de devenir une cause de justification pour le pirate malveillant qui se serait fait prendre.

A terme, nous pensons que ces manières de faire devraient vider de son sens l'idée d'une contribution au Bien de l'Humanité, les hackers « purs » employant les mauvaises méthodes et les pirates informatiques utilisant cette justification à outrance.

---

[309] Cf. supra.

c) Les motivations d'ordre politique

Les principales motivations d'ordre politique sont « l'hacktivisme » et le cyberterrorime.

1°) L'hacktivisme

Créé à, partir des mots «hacking » et «activisme » par le groupe Cult of the Dead Cow en 1994[310], l'hacktivisme poursuit principalement des objectifs politiques. Certains objectifs peuvent être de nature économique, mais la finalité est toujours politique, comme par exemple les attaques subies par les sites Amazon.com ou Yahoo.com[311].

Les objectifs des hacktivistes peuvent être variés, comme la destruction de sites pédophiles ou l'altération de sites prônant le racisme, ou d'une manière plus générale le respect de la liberté d'information[312].

Les actions des hacktivistes sont toujours très bien coordonnées, pouvant parfois nécessiter la contribution de plusieurs milliers d'internautes (comme ce fut le cas lors de l'attaque concertée vers les sites commerciaux cités plus tôt).

Aux détracteurs de ce type d'actions, qui évoquent l'illégalité et le manque de légitimité, les hacktivistes répondent qu'il s'agit *« d'un moyen de communication »*[313], ou encore que *« ce n'est pas du hacking, c'est de la communication »*[314]. D'ailleurs, la plupart des hacktivistes ne se considèrent pas comme des criminels mais bien comme des Robins des bois du réseau[315], défendant les pauvres contre les puissants.

Mais, une fois de plus, le principal problème avec l'hacktivisme, outre les dégâts qu'il peut causer, vient du fait que les hackers sont les seuls à juger, selon leur vision du monde, qui mérite d'être puni. Dès lors, si certaines motivations sont compréhensibles (comme la défense des droits de l'Homme) – sans pour autant cautionner les méthodes utilisées–, d'autres le sont beaucoup moins (par exemple, le fait, pour le groupe ®™ark[316], d'avoir altéré plus de 80000 copies d'un jeu vidéo, parce qu'ils le considéraient comme trop violent[317]), la frontière entre les Corsaires[318] (et les Whites Hats) et les « dictateurs du réseau » étant parfois très floue.

---

[310] Voir le site de ce groupe à l'adresse www.cultdead.cow.com

[311] Les hacktivistes ont considéré que ces sites, symboles de la nouvelle économie, avaient dénaturé l'esprit de l'Internet (la circulation et l'échange d'informations) pour le réduire à son aspect commercial. Ces sites se sont ainsi vus sanctionner, les hacktivistes du monde entier ayant saturé les serveurs de ces sociétés, paralysant ainsi leurs activités pendant plusieurs heures.

[312] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, p. 55

[313] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, p. 55

[314] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, p. 55

[315] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 57 et suiv.

[316] Voy. le site du groupe www.rtmark.com

[317] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, p. 59.

[318] Pour rappel, il s'agit de hackers offrant leurs services et leurs compétences aux autorités.

2°) Le cyberterrorisme

Les organisations terroristes ont recours depuis plusieurs années déjà à l'informatique pour stocker et transmettre les données relatives à leurs actions, ainsi que pour assurer la propagande relative à la cause qu'ils défendent. Ainsi, PC, disquettes, CD-Roms,… sont régulièrement saisis au cours des perquisitions effectuées pendant les enquêtes contre des organisations comme ETA, l'IRA, ou certains mouvements islamistes[319].

De plus, l'Internet est devenu une sorte de grand marché du terrorisme, où l'on peut trouver des sites expliquant en détails comment concevoir des bombes avec des produits facilement disponibles dans le commerce[320], comment réaliser des armes pour tuer, et même les meilleurs moyens techniques et juridiques pour contrecarrer les actions des autorités[321].

Le cyberterrorisme[322] s'exprime de deux manières. D'une part, il peut s'agir d'attaques physiques contre les systèmes d'informations. A ce titre, l'attentat du World Trade Center en 1993 est considéré comme l'un des premiers actes de terrorisme informatique. En raison de l'importance des dégâts matériels, plusieurs centaines d'entreprises subirent des pertes dont le total est estimé à plus de 700 millions de dollars[323]. D'autre part, il peut s'agir d'attaques logiques, comme l'envoi de trojans, virus,… contre des sites gouvernementaux ou militaires[324].

Cet aspect du cyberterrorisme s'apparente fortement à ce que l'on désigne par « cyberwar »[325], (« guerre des réseaux »).

Sur ce dernier point, il nous faut préciser que des actions de cyberterrorisme/cyberwar peuvent parfois être commandées directement par les états eux-mêmes.

A ce titre, les rapports ambigus liant les états et les pirates ne datent pas de l'avènement des nouvelles technologies. Dès le 17e siècle, à la grande époque de la piraterie (maritime), lorsque s'affrontaient corsaires espagnols, anglais, français, hollandais, les souverains louaient déjà les services

---

[319] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 69 et suiv.

[320] L'un de ces sites a pour adresse http://come.to/anarchy. On y trouve, entre autres, deux des plus célèbres « manuels de terrorisme » : l'« anarchist cookbook » et le « terrorist cookbook ».

[321] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 69 et suiv.

[322] Le cyberterrorisme ne sera abordé ici que dans son acception de « motivation » pour les criminels informatiques, et son analyse sera donc nécessairement réduite à ces considérations.

[323] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 69 et suiv

[324] Strategic road, www.strategic-road.com

[325] La cyberwar concerne les attaques logiques contre les systèmes informatiques (virus, de bombes logiques,…) mais également les actes de propagande, de désinformation,… l'ensemble de ces attaques étant perpétrées sur ou via les réseaux.

de certains d'entre eux, afin de protéger les routes maritimes, … mais également de perpétrer des actes de piraterie à leur profit[326].

Les gouvernements actuels ne font finalement que reproduire ce schéma : combattre les hackers, mais également perpétrer des actions de hacking.

De plus, ces manœuvres ne sont pas nécessairement secrètes. Ainsi, le gouvernement Chinois serait désireux de recruter des informaticiens civils afin de former, dans les écoles militaires, des escadrons de hackers[327]!

Compte tenu des moyens existant sur le marché, en vente libre, avec des investissements ridicules par rapport aux dégâts causés par les armements classiques, il est désormais possible pour un particulier, un petit pays de mettre à genoux les infrastructures d'une grande puissance ou d'une multinationale. Le cyberterrorisme peut donc, tout comme le terrorisme traditionnel, être considéré comme l'arme des pauvres, l'équipement de base du terroriste informatique se limitant à un ordinateur équipé d'un modem, le savoir faire pouvant, comme nous venons de le dire, être directement puisé sur le Net.

Un exemple des capacités offertes par les nouvelles technologies à ce type de malveillance nous est donné par le Ministère de la Défense américain, qui réunit périodiquement les plus hauts responsables de la sécurité nationale et les industriels concernés. Ensemble, ils établissent des simulations d'attaques cyberterroristes, dont voici l'un des scénarios les plus récents[328] : *« L'Iran tente de tarir la production de pétrole de l'Arabie Saoudite. Washington envisage d'envoyer des troupes dans la péninsule. Les Iraniens, se souvenant de l'échec de Sadam Hussein, décident de porter le combat sur le sol américain et de s'attaquer à son point faible : les systèmes d'information. Tout à coup des centraux téléphoniques de bases militaires deviennent inutilisables, comme saturés (virus autorépliquant), d'autres sont hors service (bombe logique). La Maison-Blanche envoie du matériel militaire dans le golfe Persique. Un train convoyant du matériel militaire destiné à partir pour l'Arabie vers un aérodrome militaire déraille suite à un problème du système de contrôle ferroviaire. Plusieurs centres météo tombent en panne. Les avions sont cloués au sol. La Banque centrale découvre une tentative de sabotage de son système de transfert de fonds. CNN annonce que l'Iran a payé des informaticiens russes et des programmeurs indiens pour détruire l'économie occidentale. Les cours des bourses de New York et Londres s'effondrent. Plusieurs banques d'importance sont piratées. L'information s'ébruite. Panique chez les épargnants qui veulent à tout prix récupérer leur argent. On signale aussi des programmes pirates de propagande sur les chaînes de télévision. Au même moment Washington est privé de téléphone (même les mobiles), il est alors très difficile pour le Président*

---

[326] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 31 et suiv.

[327] Cette information, provenant du « Quotidien de l'Armée de libération », est citée sur le site d'informations relatives à l'Internet et aux réseaux www.Internet.com.

de réunir ses conseillers. L'ordre de départ des soldats vers l'Arabie est donné, mais ce dernier s'effectue dans le plus grand chaos en raison des problèmes de communication dans les bases de déploiement… »

Ces divers travaux ont permis de déterminer les secteurs clés à protéger particulièrement (l'énergie, les transports, les télécommunications, les finances, les services d'urgence et les services publics en général) prouvant ainsi combien la menace cyberterroriste est à prendre au sérieux.

---

[328] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 70 et suiv.

D. LE CHOIX RATIONNEL DE BECKER ET L'INNOVATEUR DE MERTON

Que les motivations du hacker soient idéologiques, politiques, intellectuelles ou encore financières, elles nécessitent toutes un certain temps de préparation. Durant cette phase de préparation, le hacker va envisager ses possibilités de succès, les renseignements dont il aura besoin, mais il aura également la possibilité de tout arrêter et de revenir en arrière. Il n'agit donc pas sur impulsion et s'il se décide à « hacker » un système, il le fait en connaissance de cause.

Dès lors, le criminel informatique va recourir à ce que Bentham appelait le « calcul de félicité » et Becker, le « choix rationnel ».

C'est à Becker que l'on doit la transposition de la théorie micro-économique du choix rationnel au comportement délinquant[329]. Schématiquement, le paradigme est le suivant : le délinquant, selon un comportement calculateur, va faire la balance, entre d'une part, les risques qu'il encourt à délinquer, et d'autre part, les avantages qu'il va pouvoir en tirer.

Si cette théorie peut s'appliquer à de nombreuses formes de délits, elle est particulièrement prégnante pour la criminalité informatique, à une époque où tout devient numérique et accessible à chacun, facilement.

La théorie du choix rationnel est liée à celle des opportunités. L'opportunité se définit comme étant *« la réunion, en un lieu et à un moment donné, des circonstances matérielles favorables à la réussite d'un délit »* [330].

Il va de soi que plus la valeur de la cible est élevée, plus l'opportunité sera intéressante. De plus, la proximité et la vulnérabilité de la cible pourront également générer des occasions, et partant, des opportunités pour le criminel informatique. L'Internet ayant considérablement réduit le problème posé par la distance spatiale entre la victime et le hacker, la vulnérabilité de la cible sera alors, est-il encore besoin de le préciser, fonction des mesures de sécurité dont elle bénéficiera. Il s'agira principalement de prévention situationnelle, comme nous le verrons plus tard.

Concernant la théorie des opportunités, il nous semble utile de pointer l'aspect de facilité proposée par les nouvelles technologies.

Pour Cusson, l'opportunité constitue *« la rencontre entre un désir et un moyen de le satisfaire »*[331]. En suivant cette théorie, il nous paraît clair que le fait d'avoir à disposition une base de données gigantesque (Internet) accroît le risque de passage à l'acte délictueux.

C'est exactement ce qu'explique « Ben », un phreaker. Ainsi, lorsqu'on lui demande comment il a commencé, il déclare : *« C'est tout bête. Je suis tombé sur Internet sur une technique qui*

---

[329] G., BECKER, « Crime and punishment : an economic approach», Journal of political economy , 1968, pp. 169 à 217.
[330] M., CUSSON, *Croissance et décroissance du crime*, Paris, PUF, 1990, p. 74.
[331] M., CUSSON, *Croissance et décroissance du crime*, Paris, PUF, 1990, p. 78.

expliquait comment frauder dans les cabines téléphoniques. Le jour où j'ai eu un problème avec ma carte, je me suis dit « Pourquoi pas ? ». Après, je me suis nourri de la Toile pour améliorer mes connaissances. Enfin, j'ai reçu pas mal de conseils par mail et par chat »[332].

Il nous semble donc que la simplicité *crée* l'opportunité. Selon Cusson *« tout indique que la plupart des délinquants ont tendance à se laisser ballotter par les circonstances. Si les occasions sont nombreuses et intéressantes, la fréquence de leurs activités délictueuses a toutes les chances d'augmenter. De plus, il n'est pas exclu que le niveau d'aspiration des délinquants soit affecté par la fréquence des opportunités (…) ? Ce que nous savons de la psychologie des délinquants nous autorise à conclure qu'une augmentation des occasions les conduira à commettre un plus grand nombre de délits »*[333].

Le criminel informatique ne devra dès lors, la plupart du temps[334], plus se poser la question de savoir s'il a *l'opportunité* de commettre le crime, mais seulement s'il *veut* le commettre, si les avantages qu'il peut tirer du crime sont *suffisamment* intéressants au regard des risques encourus.

Ces théories ont principalement été critiquées en raison du fait qu'elles négligent les autres facteurs pouvant amener l'individu à délinquer. En matière de criminalité informatique, nous pensons que ces critiques sont moins pertinentes[335]. En effet, étant entendu qu'un criminel informatique peut agir par vengeance, par désoeuvrement, ou par ennui, en raison d'une situation familiale ou sociale précaire,… il n'en reste que le facteur déterminant sera l'opportunité à commettre le crime, et surtout, comme nous le verrons, la facilité avec laquelle celui-ci pourra être commis. Si une personne est tentée de commettre une infraction classique, quelques soient ses motivations ou les facteurs l'amenant à vouloir commettre celle-ci, elle pourra se voir arrêter par l'impossibilité de commettre son crime, pour des raisons matérielles par exemple. Par contre, la facilité d'action offerte par la criminalité informatique balayera généralement les obstacles qui pourraient survenir, le choix rationnel étant dès lors déterminant dans la commission de l'acte délinquant.

Enfin, la théorie des opportunités nous amène à parler de la théorie développée par Merton[336]

Pour lui, la structure sociale est constituée de 2 entités : les buts culturels et les moyens légitimes. Il explique que quand il y a une disjonction entre les buts et les moyens, la tension qui en résulte conduit à un affaiblissement de l'engagement des hommes envers les buts et les moyens, et ceux-ci se retrouvent alors dans une situation d'anomie.

---

[332] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, p. 19.
[333] M., CUSSON, *Croissance et décroissance du crime*, Paris, PUF, 1990, p. 80.
[334] Nous visons ici les criminels informatiques ayant une certaine expérience.
[335] P., MARY, *Délinquant, délinquance et insécurité. Un demi-siècle de traitement en Belgique*, Bruxelles, Bruylant, 1998, p. 683 et suiv.
[336] Cette théorie ne sera abordée ici que de manière concise.

Merton va alors présenter un tableau représentant les façons logiquement possibles de s'adapter à ce déséquilibre, les individus rejetant ou acceptant les buts culturels et/ou les moyens légitimes.

	Buts culturels	***Moyens légitimes***
Le conformiste	acceptés	acceptés
L'innovateur	acceptés	rejetés
Le ritualiste	rejetés	acceptés
Le retraitiste	rejetés	rejetés
Le rebelle	acceptés et rejetés	acceptés et rejetés

Le conformiste sera celui qui adhère aux valeurs, à la culture et aux moyens. Il assure ainsi la stabilité de la société.

L'innovateur sera celui qui adhère aux buts de la société, mais qui utilisera des moyens illégitimes pour atteindre ces buts.

Le ritualiste sera celui qui sacralise les normes et les moyens légitimes de manière outrancière.

Le retraitiste sera celui qui se retire de la société, comme les vagabonds par exemple.

Enfin, le rebelle détournera les buts et les moyens pour en créer d'autres[337].

Il nous paraît clair que le pirate informatique constituera la figure même de l'innovateur, qui utilise des moyens détournés comme le hacking pour parvenir à son but, quel qu'il soit.

Le cyberterroriste et, dans une certaine mesure, l'hacktiviste pourront, quant à eux, être comparés au rebelle, rejetant l'ordre établi pour instaurer ses propres valeurs, avec ses propres moyens que sont le piratage informatique et ses dérivés.

[337] R., MERTON, *Eléments de théorie et de méthode sociologique*, Paris, Plon, 1965, pp. 167 et suiv.

E. CONCLUSION

Plutôt de que revenir sur le profil-type ou la typologie de Donn Parker dont nous avons déjà pointés les faiblesses, nous avons choisi de conclure cette partie en insistant particulièrement sur les motivations des hackers.

Il apparaît clairement que les motivations des hackers sont la conjonction de plusieurs facteurs, comme dans toute forme de criminalité, mais certains de ceux-ci se verront modifiés par la nature « informatique » du crime. C'est le cas de la distance séparant victime et auteur ou encore de la facilité de perpétration et de préparation de l'acte.

C'est cette configuration unique qui rend la criminalité informatique si préoccupante : quelques soient leurs motivations, les délinquants informatiques ont toujours la possibilité de passer à l'acte, l'informatique diminuant fortement les contraintes spatiales et logistiques qui pourraient les décourager.

Dès lors, si la connaissance des motivations des hackers par les autorités policières peut être utile, elle ne nous semble pas pour autant déterminante. Elle pourra peut-être donner des indications sur la personnalité du hacker, ou du moins sur son modus operandi (l'hackitivisme ne recourant pas, par exemple, aux même méthodes que le hacker désireux de détourner un transfert de fond), mais, par contre, elle ne permettra pas toujours de déterminer si l'infraction est le fruit d'une personne seule ou si elle a été commise en groupe (à moins, bien sûr, que le méfait ne soit signé ou revendiqué).

D'une part, les objectifs poursuivis peuvent autant motiver le hacker solitaire que des groupes de hackers, et, d'autre part, comme nous l'avons vu, la relative facilité de perpétration des crimes informatiques ne nécessite pas d' importants moyens humains et matériels.

Dès lors, nous pensons que l'établissement de la motivation de l'auteur de l'infraction sera un élément parmi d'autres permettant d'aboutir à son arrestation, mais non déterminant à lui seul.

Quant aux théories du choix rationnel et des opportunités, elles seront déterminantes quant au type d prévention envisagée pour lutter contre la criminalité informatique, à savoir la prévention situationnelle. Nous reviendrons plus tard sur ces théories dans la partie qui lui est consacrée.

Conclusion quant aux caractéristiques des hackers

En titre de conclusion de cette partie consacrée aux caractéristiques des hackers, nous allons souligner l'importance de celles-ci et de leur étude dans l'élaboration de moyen mis en place afin de lutter contre la criminalité informatique.

La première section, concernant les différentes catégories de hackers, a permis de mettre en lumière que le hacker n'est pas toujours l'informaticien doué présenté par les médias. La majorité d'entre eux ne sont que des script-kiddies ou des lamers pour les plus mauvais, des wannabes pour les plus prometteurs.

L'importance de cette classification est double.

D'une part, elle va permettre aux hackers de se structurer en « bons et mauvais » hackers, en pirates doués et pirates se contentant de plagiats. Cette structure est importante car elle est le signe que le mouvement des hackers est un mouvement établi comme une véritable société, avec ses anciens, ses chefs, reconnus, respectés et désignés par leurs pairs, les Elites ; ses jeunes, les Script-Kiddies, les Lamers et les Wannabes ; ses «policiers », les Corsaires ; et ses délinquants, les Crackers et les Black Hats.

D'autre part, ces catégories permettent de souligner que l'aspect de facilité est un des éléments-clés des infractions informatiques. Si n'importe quel script-kiddies est capable, sans connaissances informatiques autres que celles glanées ci et là sur le Web, de commettre une infraction informatique, les mesures de prévention, et de répression, devront avant tout se focaliser sur cet aspect de facilité. Car une des différences essentielles du crime informatique avec les autres formes de délinquance est le fait que celui-ci peut être exercé par (presque) n'importe qui et avec très peu de moyen, au contraire de certaines infractions comme le terrorisme ou le braquage de banque[338].

Bien entendu, seuls les hackers les plus doués seront capables des plus gros «coups », mais les autres seront déjà capables de causer beaucoup de dégâts.

La deuxième section concerne les fondements idéologiques du monde des hackers. Ceux-ci, notamment l'importance accordée au «hacking spirit », à la TAZ ou encore à l'underground, sont autant de preuves d'une véritable culture des hackers, permettant aux pirates de se structurer, de se reconnaître entre eux, de se définir par rapport aux autres hackers et par rapport à la société en général, et de se démarquer ainsi de l'image souvent réductrice présentée par les médias. Les

[338] Nous parlons ici de manière générale, étant entendu que certaines infractions ne nécessitent pas de connaissance et/ou de moyens particuliers, comme celle relevant de la délinquance urbaine par exemple.

différents manifestes, tracts et autres déclarations, caractéristiques des pirates informatiques, terminant de revendiquer leurs différences.

L'analyse et la connaissance d'éléments comme leur conception du Bien et du Mal ou le caractère éthique sous-tendant certaines de leurs démarches seront également déterminantes dans l'élaboration de moyens préventifs et répressifs efficaces. Il ne servirait en effet à rien de systématiquement sanctionner les pirates informatiques si ceux-ci ne comprennent pas la gravité et la dangerosité de leurs actes (nous ne visons ici que les hackers « purs », et non les crackers ou black hats, parfaitement au courant de la nature de leurs délits), de la même manière que les infractions commises par un handicapé ou un enfant seront appréciées différemment que si elles avaient été commises par des adultes « normaux ».

Le but n'est pas ici de comparer les hackers à des handicapés et d'excuser les actes néfastes qu'ils pourraient poser, mais bien de souligner l'importance des notions d'éducation, de formation, dans les mesures préventives à mettre en place, sous peine de les voir se révéler inefficaces. Certes, il sera toujours possible de sanctionner pénalement les hackers, mais le but de la répression n'est pas uniquement de punir, mais, à notre sens du moins, également de dissuader les candidats délinquants.

Enfin, la troisième section consacrée aux profils et motivations des hackers poursuit le même objectif. Outre l'absence d'un profil-type du pirate informatique, l'analyse de ces motivations a permis de démontrer que, si, celles-ci étaient aussi nombreuses qu'il existait de pirates, elles sont toutes le fruit d'un calcul rationnel. Ici aussi l'aspect de facilité a été souligné, celui-ci créant véritablement l'opportunité à commettre l'infraction.

Ce calcul rationnel et la théorie des opportunités sont également déterminants car ils entraînent une réponse préventive situationnelle, avec les avantages et désavantages que celle-ci suppose. Ceux-ci seront abordés plus tard, après avoir terminer cette partie consacrée aux phénomène des hackers en présentant l'arsenal dont ils disposent.

Titre III – L'arsenal des hackers

Sans entrer trop dans des détails techniques, il nous semble intéressant d'aborder quelques unes des « armes » à la disposition des hackers.

Nous aborderons ainsi d'abord les virus et leurs familiers, avant de nous intéresser à un aspect moins connu du hacking mais indispensable à tout « bon hack », l'ingénierie sociale.

Section 1 - Virus, vers et trojans

Depuis l'avènement de l'informatique, les virus constituent certainement la plus grande crainte de ses utilisateurs. Cette crainte est d'ailleurs pleinement justifiée à la lecture des chiffres concernant le nombre de virus et leur rapidité d'expansion[339].

S'il désignait, à l'origine, le sperme et la semence des animaux et des végétaux, le terme « virus » fera son apparition en médecine au XVIe siècle pour désigner le pus, puis par extension, une source d'infection, pour finir par désigner, au XVIIe siècle, le micro-organisme responsable du mal[340].

Au début des années 1960, il s'enrichit d'un nouveau sens, celui de facteur de perturbation des systèmes militaires[341].

Ce n'est qu'en 1981 qu'il commencera à prendre son acception informatique actuelle, « Elk Cloner » étant le premier virus développé pour infecter les machines phares du moment, à savoir les Apple II. Quelques années plus tard, David Cohen, un étudiant de l'Université de Californie, désireux de créer un programme parasite – sans intention de nuire –, sorte de vie artificielle autonome comparable à celle de virus biologiques, capable de se reproduire et de pervertir les programmes, lui attribue définitivement le qualificatif « informatique » (« computer virus »)[342].

Parmi les sept étapes du cycle de vie d'un virus (création, gestion, duplication, activation, découverte, assimilation et éradication), c'est certainement la création et la duplication qui sont les plus spectaculaires. Ainsi, si en 1988 on ne comptait qu'une dizaine de virus répertoriés, ce sont désormais plus de 70000 virus qui sont en circulation. Quant à sa duplication, les progrès de l'Internet et le développement de l'entreprise en réseaux y sont pour beaucoup. En effet, si l'entreprise augmente sa portance, sa visibilité, sa flexibilité,… elle multiplie d'autant les points d'entrée et les failles accessibles

---

[339] Nous renvoyons à la partie consacrée aux faits marquants de l'histoire du hacking, plusieurs chiffres concernant les virus y étant cités.

[340] B., CLOUGH, P., MUNGO, *La délinquance assistée par ordinateur - La saga des « hackers », nouveaux flibustiers « high tech »*, Paris, Dunod, 1993, pp. 82 à 83.

[341] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 133 et suiv.

[342] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 133 et suiv.

aux virus. Ainsi, pour ne citer qu'un exemple, dans le cas du télé-travail, plutôt que de s'attaquer directement au site de l'entreprise visée, le créateur de virus va le lâcher dans l'ordinateur (personnel) d'un de ses employés, qui, lorsqu'il se connectera à son entreprise, contaminera celle-ci[343].

Il faut également noter que tous les virus n'ont pas pour vocation de nuire ou de détruire. Ainsi, la société de jeux vidéo SEGA avait créé un virus dans l'un de ses jeux qui, s'il s'avérait être piraté, affichait sur l'écran le message suivant : *« Si je suis un hacker, me voilà en difficulté. D'un autre côté, si j'avais acheté ce jeu légalement, je n'aurais pas eu de problèmes. (…) »*[344].

De même, il existe des virus « inoffensifs », comme le virus « Diana » qui se contentait d'afficher les paroles de la chanson d'Elton John « Candle in the Wind ».

Intéressons-nous maintenant aux différentes formes que peuvent prendre les virus.

A. LES GRANDES FAMILLES DE VIRUS

Défini en informatique comme étant un programme dont l'objectif principal est d'altérer, d'endommager ou de détruire un système informatique, le virus peut porter plusieurs appellations, en fonction de son action ou de son mode de contamination[345].

Le virus vise trois cibles potentielles : les programmes, le système à proprement parler, et/ou les macros-instructions (que l'on trouve dans les programmes de traitement de texte ou les tableurs).

Du plus bénin (le virus «Diana ») au plus offensif (les virus utilisés par les crashers et visant la destruction complète des fichiers), les virus peuvent être regroupés en trois grandes familles.

1) Les vers

S'auto-reproduisant à l'infini et se déplaçant au travers de n'importe quel réseau (Internet, Intranet d'entreprise, réseau local,…), le ver est le virus des réseaux par excellence.

Le ver présente l'avantage d'être un agent autonome capable de se propager sans l'utilisation d'un programme quelconque ou, mieux, d'un support physique[346]. C'est cette dernière caractéristique qui lui permet de se déplacer si facilement, par l'intermédiaire des courriers électroniques par exemple.

---

[343] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 133 et suiv.
[344] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 133 et suiv.
[345] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 133 et suiv.
[346] Sécurité Internet, www.2si.org.

Ainsi, avec le développement des messageries électroniques, les vers ont connu un développement explosif ces dernières années, le ver « I Love You » ayant par exemple contaminé 48 millions d'internautes en l'an 2000.

2) Les trojans

« Brisés par la guerre, repoussés par les destins, les chefs des Grecs, après tant d'années écoulées, construisent sous la divine inspiration de Pallas un cheval haut comme une montagne dont ils forment les côtes de sapins entrelacés. C'est, prétendent-ils, une offrande à la déesse pour un retour heureux ; et le bruit s'en répand. Une élite de guerriers tirés au sort s'enferme furtivement dans ces flancs ténébreux ; et le ventre du monstre jusqu'au fond de ses énormes cavernes se remplit de soldats armés » (Virgile, *Énéide*, II, v. 13-20). La technique informatique du cheval de Troie obéit strictement aux enseignements helléniques.

Le trojan, ou «cheval de Troie », est un programme qui se cache dans un autre programme apparemment en « bonne santé »[347]. Il ne se déclenche que lorsque l'application porteuse est lancée, si bien que le simple fait de posséder un fichier infecté par un trojan ne suffit pas à activer celui-ci.

Une fois lancé, le cheval de Troie peut accomplir plusieurs actions : vol de mots de passe, copie de données, destructions diverses,… Mais son utilisation la plus courante reste la création de failles de sécurité dans un réseau pour autoriser d'autres personnes à s'y introduire[348].

A la différence des autres virus, les trojans ne se reproduisent pas et ne nécessitent pas de grandes connaissances pour les utiliser, si bien que l'un des trojans les plus connus actuellement, Back Orifice 2000, permet à nombre de lamers et autres script-kiddies de se faire la main.

3) Les bombes logiques

Ce type de virus s'installe sur un ordinateur et attend un signal externe pour exploser et causer d'énormes dégâts[349].

La particularité des bombes logiques provient du fait qu'elles doivent être installées « physiquement » sur la machine cible, ce qui explique qu'elles constituent les outils de vengeance de prédilection des employés licenciés.

La bombe logique, une fois installée, attendra son déclencheur. Il pourra s'agir du lancement d'une application, du passage à une heure précise, à une date déterminée,…

Enfin, après avoir défini ce qu'étaient les virus informatiques, il nous semble opportun de dire un mot sur leurs créateurs.

---

[347] Sécurité Internet, www.2si.org.

[348] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 140 et suiv.

B. LES CRÉATEURS DE VIRUS

Les créateurs de virus sont-ils encore des hackers (au sens de « l'esprit du hack »)[350] ? A la lecture du rapide historique qui vient d'être exposé, et de la disparité existant entre les virus et l'utilisation qui peut en être faite, cette question nous semblait pertinente, les virus découlant, au départ, tout comme le hacking, d'une curiosité scientifique et non d'une volonté de nuire.

Pour Danielle Kaminsky, auteur d'une étude de 3 ans réalisée pour le Clusif[351], les créateurs de virus et les hackers[352] présentent quelques similitudes. Tout comme les hackers, il n'y a pas de profils-type du créateur de virus. Ils ont une vie sociale « normale », ont des amis, pratiquent le sport, la musique. Ils pratiquent différentes professions, allant du responsable informatique aux professions littéraires et artistiques.

Comme les hackers, assez logiquement, ils présentent un intérêt marqué pour les nouvelles technologies et pour l'informatique en particulier.

A contrario, il se démarque du hacker principalement pour deux raisons. Tout d'abord, le créateur de virus n'a pas réellement de cible, car à l'exception (éventuellement) du premier ordinateur infecté, il ne contrôle pas la propagation de son virus, alors que le hacker a, quant à lui, une cible précise. Ensuite, le créateur de virus n'a qu'un souhait : que sa création contamine le plus d'ordinateurs possible, alors que le hacker ne vise lui qu'à pirater sa cible dans le respect de l'esprit du hack. Enfin, le créateur de virus ne vise que son seul plaisir, au contraire du hacker qui est porté par des motivations dépassant son seul plaisir et donc sa seule personne, afin, selon lui, de participer à édifier les fondements de l'information libre pour tous et aux progrès de l'Humanité[353].

Selon Kaminsky, il semblerait donc que les créateurs de virus ne soient pas des hackers « purs », leurs intérêts respectifs divergeant complètement.

Il n'en reste qu'une fois encore, une classification n'est pas aisée, certains hackers « purs » créant des virus afin de réaliser leur hack. Mais cela, tout le monde s'en sera douté.

Contrairement aux virus qui ne sont utilisés que par certains hackers, il existe une « arme », ou plutôt un outil, que tous les hackers, sans exception, se doivent de maîtriser : l'ingénierie sociale.

---

[349] Y., CHATELAIN, L., ROCHE, *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000, pp. 140 et suiv.
[350] Nous visons ici les créateurs actuels de virus, et non les pionniers comme David Cohen.
[351] D., KAMINSKY, *Auteurs de virus, entreprises, éditeurs d'antivirus : les liaisons dangereuses*, Paris, CLUSIF, Octobre 1998.
[352] Nous visons ici les hackers « purs ».
[353] Ces informations proviennent du site www.zataz.com/zatazv7/dk.htm, où Damien Bancal a réalisé une interview de Danielle Kaminsky.

Section 2 - L'ingénierie sociale

Le crime informatique, comme d'autres formes de criminalité, repose sur cinq postulats de base[354] :

- Tout système informatique est vulnérable et comporte des failles ;
- Toute personne ayant accès à un système informatique est susceptible de découvrir ces failles ;
- Quiconque découvre ces failles peut être tenté de les utiliser à son profit ;
- Si les risques sont faibles, ces failles seront utilisées ;
- Ces failles seront d'autant plus facilement utilisées que l'on opère de l'intérieur de l'entreprise ;

Malgré les nombreuses barrières techniques destinées à protéger les systèmes d'informations[355], les hackers continuent à s'introduire dans les ordinateurs et les réseaux.

La clé de leurs succès est le « social engineering » ou « ingénierie sociale »[356].

Cette technique essentielle pour obtenir certaines informations ou convaincre certaines personnes, correspond à une sorte de sous-produit du hacking et tout bon hacker se doit de la maîtriser.

L'ingénierie sociale est un terme utilisé par les hackers pour désigner une technique d'intrusion sur un système qui repose sur les points faibles des personnes qui sont en relation avec un système informatique. Le but est de piéger les gens en leur faisant révéler leur mot de passe ou tout autre information qui pourrait compromettre la sécurité du système informatique[357].

Les hackers font ainsi croire à leur interlocuteur qu'ils font partie du service de maintenance de la compagnie du téléphone, ou encore qu'ils sont administrateurs réseaux, afin de soutirer leurs codes d'accès.

De par leurs études des systèmes informatiques et leurs connaissances des réseaux, ils n'ont aucun mal à se faire passer pour un professionnel, utilisant le jargon adéquat, que ce soit celui de l'informatique, des télécommunications ou encore de la bureautique[358].

L'ingénierie sociale peut prendre plusieurs formes.

Elle peut ainsi être « basique », le hacker ne cherchant même pas à préparer son arnaque et appelant un employé de la société visée au hasard.

---

[354] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, pp. 212 et suiv.

[355] Nous reviendrons sur ces techniques plus tard dans la partie consacrée à la prévention.

[356] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, pp. 212 et suiv.

[357] Sécurité Internet, www.2si.org.

[358] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, pp. 212 et suiv.

Dans d'autres cas, les hackers vont jusqu'à fouiller dans les poubelles afin d'obtenir des informations sur l'organigramme de la société, sur les responsables de la sécurité informatique,… Ils chercheront ainsi à avoir le plus d'informations sur leurs « cibles », afin de deviner le mot de passe de ces dernières (par exemple le prénom de leurs enfants, leur date d'anniversaire,…).

Enfin, certains n'hésitent pas à se faire engager comme concierge, veilleur de nuit, ou tout autre fonction qui leur permettra d'accéder à de nombreuses informations utiles sans éveiller les soupçons.

L'ingénierie sociale, outre son caractère « utile », offre une satisfaction non négligeable pour tout hacker : elle lui permet de berner son interlocuteur.

Cette idée est à la base de l'ingénierie sociale, ainsi que de nombreux cas d'intrusion (c'est d'ailleurs une des raisons souvent invoquée, à tort ou à raison, par les cybercriminels pour expliquer leurs actes[359]).

Ainsi, contrairement à ce que l'on pourrait peut-être penser, ce ne sont pas tant les virus et autres programmes informatiques d'intrusion qui font de vous un véritable hacker que la maîtrise parfaite de l'ingénierie sociale.

Si la manipulation des trojans est parfaitement accessible à n'importe quel script-kiddies, l'ingénierie sociale nécessite quant à elle des connaissances plus approfondies, dans de nombreux domaines, démontrant ainsi que les hackers « purs » sont plus que de simples informaticiens doués, passionnés au point de risquer de se faire prendre au sein-même de l'entreprise, l'institution visée.

Enfin, il est évident que la maîtrise de l'ingénierie sociale par les hackers sera la première cause d'échec des mesures de prévention mises en place, comme nous allons le voir à présent.

[359] Pour l'exemple, nous renvoyons à la partie consacrée à Kevin Mitnick.

Troisième Partie – Les moyens de prévention en matière de criminalité informatique

Aujourd'hui, sur le plan de la prévention en matière de systèmes d'information, on préfère généralement le terme de « sécurité » à celui de « défense »[360]. On parle d'ailleurs bien de « sécurité informatique » et non de « défense informatique ».

Ce changement de termes correspond à un changement d'objectifs, de méthodes et de statut[361]. Ainsi, jusqu'à une date récente, la cryptologie, par exemple, était un domaine placé sous le contrôle de l'armée. Désormais, la guerre froide et l'existence d'une menace militaire tangible et facilement identifiable ont cédé la place à un monde aux menaces multiples et souvent imprévisibles.

Il y a désormais moins *une* menace que *des* risques, et la nécessité d'une défense immédiate se fait moins sentir qu'une sécurité à long terme.

Comme nous allons le voir, ce besoin de sécurité à long terme va se traduire en outils majoritairement techniques, caractéristiques de la prévention situationnelle. Ce sera pour nous l'occasion de déterminer les avantages, mais également les carences de ces outils, tout aussi caractéristiques de ce type de prévention.

Nous aborderons ensuite succinctement quelques solutions destinées à améliorer ces outils, comme l'éducation des jeunes et la formation du personnel.

Enfin, nous conclurons cette partie sur la prévention situationnelle en lui appliquant la théorie de la régulation économique du crime, nous permettant ainsi de pointer les véritables bénéficiaires de cette prévention que sont les sociétés de sécurité et d'audit informatiques.

---

[360] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 91.

[361] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 91.

Titre I – Prévention situationnelle et moyens techniques

Cette partie sera consacrée aux outils techniques de prévention, et donc, à la prévention situationnelle. Nous ne viserons ici que la prévention du crime informatique pur, étant entendu que l'ensemble des risques encourus par les systèmes d'information ne sont pas exclusivement de nature informatique. Comme nous l'avons vu dans la partie consacrée aux risques, le feu, l'eau, les dégâts matériels en général sont autant de risques potentiels. Ceux-ci nécessiteront des moyens préventifs spécifiques (porte coupe-feu, système d'alarme, ….) que nous n'aborderons pas ici.

Section 1 – Les outils techniques

Ne désirant pas rentrer dans des détails techniques qui nous éloigneraient de notre sujet, nous ne présenterons que trois outils, à savoir les anti-virus, les firewalls et la cryptologie, qui seront définis succinctement.

Analyser l'ensemble des outils techniques n'aurait pas de réelle utilité, le but de cette partie étant de pointer qu'il s'agit de prévention situationnelle et d'en définir les limites.

• L'anti-virus :

Comme chacun s'en doute, et sans nécessiter de plus amples informations, il s'agit d'un logiciel permettant de détecter et de « nettoyer » les données infectées par un virus[362].

• Le firewall :

Le firewall (« pare-feu ») est l'un des moyens les plus fréquemment utilisés pour se protéger, à tel point qu'il est même intégré dans le dernier système d'exploitation de Microsoft, Windows XP[363].

Il s'agit d'un logiciel faisant office de passerelle entre l'entreprise/l'ordinateur du particulier et l'Internet. Il est chargé d'interdire et d'autoriser les flux d'informations en entrée ou en sortie.

L'objectif du firewall est de protéger le réseau Internet des accès non autorisés provenant de l'extérieur. Il dispose également d'un contrôle au niveau applicatif, permettant ainsi de bloquer le recours à certains programmes[364].

• La cryptologie :

---

[362] Symantec, www.symantec.fr
[363] Microsoft, www.microsoft.fr.
[364] S., GHERNAOUTI-HELIE, *Sécurité Internet, Stratégies et technologies*, Paris, Dunod, 2000, pp. 212 et suiv.

La cryptologie est une technologie permettant de transmettre des messages ne pouvant être lus d'une manière intelligible que par le destinataire final.

L'information ainsi transformée peut transiter par des canaux publics sans que la confidentialité de la transmission ne soit remise en cause.[365]

Il existe deux méthodes de chiffrement :

- le chiffrement symétrique : la source et la destination de l'information disposent chacune de la même clé, spécifique à ce chiffrement, qui sert à crypter et décrypter le message.
- Le chiffrement asymétrique : où l'on trouve une clé publique, permettant de crypter le message, et une clé privée, que seul le destinataire détient et permettant de décrypter le message. L'intérêt de cette méthode est d'éviter de voir transiter une seule et même clé sur les réseaux[366].

Il existe d'autres moyens de protection, comme l'authentification, le filtrage de contenu, la détection d'intrusion via un NIDS (Network Intrusion Detection System),…

[365] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 179 et suiv.

[366] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 179 et suiv.

Section 2 – La prévention situationnelle

La prévention situationnelle prône des mesures concrètes et physiques de protection de la cible. Elle est utilisé pour les cas où l'acte délinquant est le résultat d'un calcul rationnel du criminel entre les avantages à commettre l'infraction et les risques qu'il encourt.

Cusson la définit comme étant *« l'ensemble des mesures non pénales qui visent à empêcher le passage à l'acte en modifiant les circonstances particulières dans lesquelles une série de délits semblables sont commis ou pourraient l'être »*[367].

Ce modèle de prévention situationnelle se basse essentiellement sur la théorie des opportunités qui consiste à faire des occasions de délinquance l'unique facteur décisif de l'action criminelle. La prévention situationnelle aura, dès lors, pour objectif de supprimer ou du moins de réduire ces occasions.

Gassin, au sujet de la prévention situationnelle, considère que *« cette approche englobe dans son sens le plus large, les divers efforts déployés pour amener les victimes éventuelles à se protéger contre le crime en réduisant l'accessibilité possible ou en faisant appel à des services privés de sécurité plutôt que de compter sur la police ou sur la modification des comportements des délinquants potentiels »*[368].

Cette deuxième définition est centrée non plus sur le délinquant, mais sur la victime, Cusson rajoutant que la mise sur pied de telles mesures implique nécessairement la participation active du citoyen et plus particulièrement des victimes potentielles[369].

Cette appréciation de la prévention situationnelle est caractéristique d'un glissement de la responsabilité de la gestion de la sécurité par l'Etat vers les entreprises et le secteur privé.

A ce titre, il nous semble que cette deuxième acception de la prévention situationnelle s'applique parfaitement à la criminalité informatique, où l'Etat, au niveau préventif, se relève généralement incapable d'assurer la sécurité des citoyens, si bien que cette mission sera dévolue aux organismes privés.

Il faut également souligner que la prévention situationnelle s'inscrit, contrairement à la prévention sociale, dans une perspective à court terme. Cette caractéristique est également applicable à la prévention de la criminalité informatique, la durée de fiabilité d'une protection informatique étant inversement proportionnelle à l'ingéniosité du pirate informatique. Afin de lutter contre cette tendance, les divers développeurs de logiciels préventifs (anti-virus, fire-walls,…), développent, le plus souvent

---

[367] M., CUSSON, « La criminologie a-t-elle un avenir ? », R.I.C.P.T., 1998, vol. XLI, n°4, p.433.
[368] R., GASSIN, « Les relations entre la prévention situationnelle et le contrôle de la criminalité », R.I.C.P.T., 1996, n°3, p. 256.
[369] M., CUSSON, « L'analyse criminologique et la prévention situationnelle », R.I.C.P.T., vol. XLV, n°2, 1992, p. 143.

gratuitement, des mise à jour de leurs produits, rendant ceux-ci « plus récents », et augmentant ainsi la fiabilité de la sécurité informatique du système[370].

Consécutivement à ce que nous avions dit concernant le calcul rationnel opéré par le délinquant informatique, la prévention situationnelle a pour but que les coûts de l'acte délictueux soient supérieurs aux bénéfices retirés de celui-ci.

La prévention situationnelle joue principalement sur trois grands axes[371] : l'augmentation des efforts à fournir par l'infracteur pour commettre le délit, l'augmentation des risques que l'infracteur potentiel devra courir et la diminution des gains résultant du crime commis.

Les outils techniques que nous venons d'aborder devraient permettre de jouer sur les deux premiers axes. En effet, la cryptologie, le firewall, l'anti-virus,… sont autant d'éléments qui vont ralentir l'infracteur. Nous employons le terme « ralentir » car, *« tout ce qui a été créé par l'Homme pouvant être détruit par celui-ci »*[372], il est utopique d'imaginer posséder un système de protection infaillible.

D'une part, il y aura toujours quelque part un hacker plus malin que les autres capable de pénétrer votre système, et d'autre part, si exceptionnellement ce n'était pas le cas, les criminels informatiques recourraient à l'ingénierie sociale pour franchir ces obstacles.

Ces deux points expliquent pourquoi la prévention situationnelle, en matière de criminalité informatique aboutit à un phénomène de déplacement[373]. Les hackers, moins doués, incapables de pénétrer un système « bien » protégé, se focaliseront alors sur un autre, plus perméable aux intrusions.

Le troisième axe confirme également ce phénomène de déplacement. Concrètement, diminuer les gains résultant du crime informatique consiste à éviter que des informations ne soient volées, copiées, par le criminel informatique. Mais, comme nous l'avons vu, notamment en raison des facilités offertes par l'Internet en matière de criminalité informatique[374], le seul véritable moyen de prévention utile est la disparition pure et simple de ces informations. A ce sujet, la cryptologie pourrait être un système efficace, mais pas à long terme. Pour l'exemple, rappelons que le réseau Echelon est capable de déchiffrer n'importe quel message, pour peu, bien entendu, qu'on lui en laisse le temps. Dès lors, la disparition des informations, ou plutôt l'inaccessibilité à celles-ci constitue la seule prévention efficace. En pratique, cela signifie que les ordinateurs contenant des données sensibles ne soient pas connectés

---

[370] Dans le cadre des anti-virus, par exemple, il s'agira d'actualiser la liste des virus existants, étant entendu que des dizaines de nouveaux virus sont créés chaque jour.

[371] R.V., CLARKE, « Les technologies de la prévention situationnelle », Cahiers de la sécurité intérieure, 1995, n°21, 3e trimestre, pp. 101 à 113.

[372] Il s'agit d'une phrase régulièrement répercutée sur les forums de discussions, encourageant les apprentis hackers à persévérer dans leurs recherches de failles des systèmes de protection.

[373] C'est également le cas pour d'autres formes de criminalité. Il s'agit-là d'un biais récurrent de ce type de prévention.

[374] Cf. supra.

sur le réseau Internet, ni sur aucun réseau en particulier (les réseaux privés comme Intranet par exemple) ; que ces données ne soient accessibles qu'à un nombre limité de personnes et que l'accès de celles-ci aux information soit également limité (badge, mots de passe,…).

Seulement, certaines entreprises ne peuvent se permettre de voir leurs données sensibles être déconnectées du réseau Internet. Prenons par exemple le cas des systèmes d'opérations bancaires à domicile (comme le Homebanking proposée par la BBL par exemple). Leur utilité perdrait tout son sens si l'accès aux informations relatives aux clients n'était pas possible. De même pour les sociétés proposant des services, des logiciels, en téléchargement : quel serait l'utilité de tels services si le contenu proposé n'était pas accessible ?

L'effet de déplacement sera donc le fait de l'un de ces deux éléments ou des deux : l'absence ou le manque de protection (technique) efficace et l'absence de contenu « intéressant » pour le pirate. Le pirate confronté à un système qu'il ne peut pénétrer s'intéressera à d'autres cibles plus accessibles, comme il le fera si les cibles visées ne contiennent pas d'informations sensibles.

A contrario, la prévention situationnelle peut avoir un autre effet pervers en ce sens que, plutôt que de décourager les hackers, elle tendrait plutôt à les stimuler, ceux-ci considérant les systèmes de sécurité mis en place comme un défi à relever. C'est par exemple le cas pour les sites du Pentagone, de la Nasa, qui sont, assez logiquement, très bien protégés, mais qui continuent de faire l'objet de milliers d'attaques chaque année[375].

Il nous semble donc essentiel d'insister sur la nécessité d'éduquer les futurs jeunes pirates informatiques. Comme nous l'avons vu, ceux-ci considèrent souvent le piratage comme un jeu, leur permettant de se valoriser, leurs parents n'étant pas toujours conscients de la portée des actes de leurs enfants. Nous y reviendrons dans un instant.

D'une manière générale, la prévention situationnelle souffre principalement du fait qu'elle ne se suffit pas à elle-même. Si elle peut être très utile dans certains cas, elle est généralement limitée par le fait que les outils techniques peuvent être détournés, manipulés, si bien qu'elle ne sera efficace que si ses utilisateurs ont pleinement connaissance des risques qu'ils encourent et donc de ce que qu'ils peuvent et ne peuvent pas faire ou dire. Ainsi, quelle sera l'utilité d'un accès par mots de passe, par exemple, si son utilisateur le communique à n'importe qui ? De même, un anti-virus, un firewall mal configuré ne servira également à rien.

[375] National Infrastructure Protection Center, (« Centre de protection des institutions nationales »), www.nipc.gov.

Sans cette connaissance des risques encourus, l'ingénierie sociale pratiquée par les hackers permettra, tôt ou tard, de venir à bout du plus sophistiqué des systèmes de sécurité informatique.

Ce qui nous amène à parler de l'importance de la sensibilisation aux risques.

Titre II – Une sensibilisation essentielle aux risques

Dans cette partie, nous allons aborder ce qui nous semble être indispensable à une politique de prévention cohérente, à savoir l'éducation et l'information.

L'éducation concernera essentiellement les jeunes, mais également, dans une certaine mesure, leurs parents, qui n'ont pas toujours conscience de la portée des actes perpétrés par leurs enfants.

Cette sensibilisation des parents ne sera possible que grâce à une information claire sur les risques informatiques, ce qui nous amènera à parler de la sensibilisation du personnel et des entreprises en général aux risques informatiques. Ce sera l'occasion de souligner une initiative belge, à savoir le « guide à destination des utilisateurs d'Internet ».

Section 1 – L'importance de l'éducation

La notion de jeu étant généralement indissociable du piratage informatique, la nécessité d'une éducation préventive fait l'objet d'un large consensus parmi les spécialistes de la sécurité informatique : *« la communauté informatique, y compris les éducateurs, se doit de promouvoir un sens éthique aux jeunes utilisant des ordinateurs. Il faut leur expliquer que le crime informatique est un crime. Nous devons détruire le « syndrome de Robin des bois » et éviter d'encourager les hackers en leur faisant de la publicité (…). Les médias devraient arrêter d'en faire des héros populaires »*[376].

Ainsi, à titre d'exemple, la société Infogrames, spécialisée dans les jeux vidéo, victime à plusieurs reprises du piratage de ses logiciels, déclarait à propos des auteurs : *« nous ne souhaitons pas qu'ils aillent en prison. Nous proposerons, par exemple, qu'ils fassent un travail d'intérêt général dans notre société, et s'ils sont vraiment géniaux, nous n'hésiterons pas à les embaucher. Mais nous voulons que les parents, les éducateurs et les « teen-agers » prennent enfin conscience qu'en piratant, on passe du jeu au vol »*[377].

Dès leur plus jeune âge, les enfants doivent être conscients de ce qu'ils font avec leur ordinateurs, et que tout ce qui est possible grâce à lui n'est pas pour autant permis.

La criminalité informatique a ceci de particulier que, contrairement à l'ensemble des autres formes de criminalité, il n'y a pas d'âge pour y entrer[378]. Elle ne nécessite pas d'acheter des armes ou du matériel sophistiqué, mais seulement un ordinateur et un modem.

Dès lors, il faut préalablement que les parents aient également compris la réelle portée des actes de piratage informatique, et qu'ils y voient, eux aussi, plus qu'un simple jeu.

Cette perception ne sera possible que grâce à une information et une représentation exacte[379] de la criminalité informatique, que ce soit par les autorités ou les médias.

A ce titre, consécutivement à ce que vient de dire Zajac, il nous semble que les médias ont un rôle déterminant à jouer dans l'éducation des jeunes.

Une véritable prise de conscience de la part des jeunes (et de leurs parents) ne sera pas possible sans cela, la représentation de certains criminels informatiques et de leurs « exploits » donnant parfois l'impression de se trouver face à des héros, tronquant ainsi l'image de la réalité de la criminalité informatique.

---

[376] B.-P., ZAJAC, « Computer Fraud in college, a case study », Securicom, 1985, p. 58.

[377] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, p.220.

[378] Il est entendu que certaines formes de criminalité sont accessibles à des jeunes (comme la délinquance urbaine par exemple), mais il est assez rare de voir un jeune de 14 ans braquer une banque, alors que nombre de script-kiddies commencent leurs activités à cet âge.

[379] Nous ne visons pas ici les statistiques criminelles, dont nous avons déjà dénoncé les biais plus tôt, mais la représentation parfois « enjolivée » des criminels informatiques par les médias.

Section 2 – La sensibilisation indispensable du monde de l'entreprise

L'analyse des risques que nous avons développée dans la première partie de cet exposé a permis de souligner l'importance du facteur humain dans les risques encourus par les entreprises.

Contrairement à ce que l'on pourrait penser, la prévention des risques informatiques n'est pas (ne doit pas) être cantonnée aux outils techniques que sont les firewalls et autres anti-virus. Le personnel a également une grosse part de responsabilités dans la facilité d'accès aux informations stratégiques, et dès lors, un grand rôle à jouer pour assurer une certaine efficacité aux moyens préventifs mis en place.

Il est nécessaire d'expliquer non seulement l'importance des outils employés, mais également, et surtout, les possibilités dont disposent les pirates. Celles-ci concernent les outils logiques, mais également les méthodes relevant de l'ingénierie sociale, si bien qu'en caricaturant, ce ne sont pas uniquement les informaticiens qui doivent être informés, mais également les concierges, surveillants de nuit et autres employés administratifs.

Ainsi, même si, quand il ne s'agit pas d'une malveillance délibérée, « l'erreur est humaine », quelques précautions peuvent néanmoins être prises[380]:

- la réactualisation permanente des procédures (de sécurité, d'utilisation,..) ;
- le changement des mots de passe après le départ des personnels les connaissant ;
- l'utilisation prudente des documents, disques ou supports quelconques dont l'origine n'apporte pas toutes les garanties de sérieux et de sécurité ;
- la prudence dans les échanges verbaux, en particulier, hors de l'entreprise (ceci dans le but de lutter contre l'ingénierie sociale) ;
- l'action personnelle des dirigeants en faveur de l'esprit de sécurité et l'exemple qu'ils doivent en donner ;
- la formation du personnel de recrutement
- …

Cette formation du personnel présente deux avantages indéniables pour les entreprises. D'une part, elle ne nécessite pas de gros investissements. C'est un argument de poids lorsqu'on se réfère aux problèmes de sécurité informatique causés par un manque de budget suffisant[381].

---

[380] F., BRACONNIER, « Criminalité et sécurité sur les systèmes d'information », Liaisons, décembre 1991, n°305, pp. 10 à 23.
[381] Cf. supra.

D'autre part, ces précautions, si elles ne sont pas infaillibles, devraient néanmoins permettre de réduire les risques, en diminuant les fuites provenant du personnel qui, comme nous l'avons vu, constitue une source déterminante d'informations pour les hackers.

Section 3 – Le « guide à destination des utilisateurs d'Internet »

En avril 2000, le ministère belge des Affaires économiques a publié le «guide à destination des utilisateurs d'Internet »[382].

Ce guide, adressé à l'ensemble des utilisateurs d'Internet, a été réalisé avec le Centre de Recherches Informatique et Droit (CRID) des Facultés Notre-Dame de la Paix de Namur.

Il a pour ambition d'aborder l'ensemble des questions auxquelles les utilisateurs peuvent être confrontés, de la connexion Internet aux achats en ligne.

Si ce guide est très bien réalisé, utilisant un langage clair et accessible à chacun, nous regrettons qu'il n'aborde que très ponctuellement les problèmes de sécurité sur le réseau[383], pour se focaliser exclusivement sur les questions d'ordre économique[384].

Bien que ce guide soit le fruit du travail du ministère des Affaires économiques et du CRID et qu'il est donc normal qu'il soit centré sur les aspects économiques du réseau, la question de la sécurité nous semble devoir être abordée à chaque fois qu'il est question d'Internet en particulier, et d'informatique en général.

Dès lors, encore plus qu'une partie plus importante consacrée à la sécurité informatique, nous regrettons qu'une initiative de ce type n'ait pas été mise sur pied par le ministère de la Justice, principal concerné lorsqu'il s'agit de sécurité informatique, et encore plus aujourd'hui qu'une loi spécifique à la criminalité informatique a été adoptée[385].

---

[382] Ministères des Affaires économiques, *Guide à destination des utilisateurs d'Internet*, éd. du CRID, avril 2000 (disponible à l'adresse http://.mineco.fgov.be/information_society/consumers/consumers_Internetguide/homefr.htm)

[383] Moins de 10 pages sur l'ensemble des 100 pages que comprend ce guide.

[384] Ainsi, une des parties du guide est consacrée à la création d'un site Internet.

[385] Il faut également noter que le Ministre de la Justice Marc Verwilghen a fait de la criminalité en col blanc une des priorités du Plan fédéral de sécurité et de politique pénitentiaire, et considère la criminalité informatique comme une sous-catégorie de celle-ci.

Conclusion : la notion de « système de crime »

Dans cette conclusion, nous tenons à revenir sur l'élément essentiel mis en place dans le cadre de la prévention, à savoir la prévention situationnelle et plus précisément les différents outils techniques qu'elle suppose.

Plusieurs criminologues ont montré que la théorie du marché économique pouvait être appliquée au crime. Ainsi, pour Erlich, le marché régule les comportements respectifs des criminels, de leurs victimes et des forces de police ou de justice chargées de faire appliquer la lois. Dès lors, lorsque la criminalité augmente, l'effort de lutte contre cette criminalité augmentera également. Cette évolution se poursuivra jusqu'à ce que le coût de protection devienne plus élevé que les économies opérées sur la criminalité. Il y a donc un niveau optimal[386].

Ce raisonnement s'applique à la criminalité informatique. L'accroissement des actions malveillantes a pour effet d'inciter les entreprises à se protéger (même si, comme nous l'avons vu, elles ne le sont généralement pas assez), jusqu'à ce que le coût de cette protection devienne disproportionné, prohibitif par rapport aux risques réels encourus.

Les dépenses de protection suivent donc la loi des rendements : le premier franc dépensé permet des gains potentiels importants, le gain marginal diminuant lorsque ces dépenses augmentent[387].

Cette idée de régulation a été reprise par Cook. Selon lui, le niveau de criminalité est directement lié aux interactions entre, d'une part, les victimes potentielles qui cherchent à adapter leur niveau de protection, et d'autre part, les criminels potentiels dont le but est de chercher des opportunités[388].

Dans le domaine de la criminalité informatique, nous voyons d'un côté les entreprises, victimes potentielles, mettre en place des moyens de prévention et de protection, et de l'autre, les hackers, espions et autres pirates adaptant leurs techniques et le choix de leurs cibles en fonction du degré de difficulté de protection de celles-ci.

Cette interaction entre les futures victimes et les délinquants fait l'objet d'une sorte de « processus de régulation dynamique » résultant de deux tendances. La première est que les victimes intéressantes auront tendance à être attaquées. La seconde est que, précisément, ces cibles seront généralement les

---

[386] I., ERLICH, « The Economic Approach to Crime, a preliminary Assessment », Criminology Review Yearbook, Sage Publications, pp. 25-60.

[387] J.-P., MOATTI, « L'économie de la sécurité, de l'évaluation à la prévention des risques technologiques », La Documentation Française, 1989, p. 27.

[388] P.-J., COOK, « The Demand and Supply of Criminal Opportunities », Crime and Justice, University Press, 1986, vol. 7, pp. 1 à 27.

mieux protégées (pour peu qu'elles aient conscience du risque encouru)[389]. C'est également le cas dans le domaine de la criminalité informatique : les opportunités les plus nombreuses se trouvent dans le secteur financier, qui se trouve également être le plus protégé. Logiquement, ce processus de régulation fera diminuer le crime pour les cibles de mieux en mieux protégées.

Ainsi, un véritable marché de la sécurité s'est développé pour répondre à ces demandes de protection. Après avoir été négligées, les sociétés de consultance en sécurité informatique sont « en plein boom »[390]. Si les précurseurs en matière de sécurité informatique furent le Clusif en France et le Clusib pour la Belgique (sous la forme d'ASBL), c'est aujourd'hui des centaines de sociétés de ce type qui ont vu le jour. A titre d'exemple, on peut citer Sequoia[391] pour la Belgique, ou Edelweb[392] pour la France.

Cette dernière présente la particularité, comme de nombreuses entreprises de consultance informatique, d'avoir été créée par un ancien hacker. Son fondateur, Paul-André Pays, est désormais passé de l'autre côté de la barrière, et lutte à présent contre ses anciens « amis ». Il a pour mission de tester et d'améliorer les défenses des systèmes informatiques, en raison des risques de plus en plus nombreux auxquels ceux-ci sont confrontés (accès généralisé à l'Internet, nomadisation croissante des salariés, connections à distance aux réseaux informatiques de l'entreprise,…)[393].

La conjonction de tous ces éléments amène à comparer la notion de « criminalité informatique », englobant ici l'ensemble des notions précédemment développées concernant les hackers, en particulier leur mode d'intégration et à leurs motivations, à la notion de *« système de crime »* développée par Cusson. Il le définit comme *« l'ensemble des relations qui lient entre eux les délinquants, les victimes potentielles, les agents du contrôle social et les agents pénaux. La dynamique de ce système repose sur trois processus fondamentaux. Premièrement, le crime varie en raison directe des profits qu'il apporte à ses auteurs. Deuxièmement, il varie en raison inverse de l'intégration et du contrôle social. Troisièmement, il provoque des réactions visant à s'en protéger et ces dernières influencent à leur tour le crime »*[394].

En conclusion, il apparaît clairement que c'est le domaine privé qui permettra l'effectivité de la prévention en matière de criminalité informatique. Que ce soit sur le plan technique ou de la formation du personnel, c'est au sein de l'entreprise que l'essentiel de la lutte devra se faire.

---

[389] P., ROSE, J.-M., LAMERE, *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996, p.234.
[390] P., BLANCHARD, *Pirates de l'informatique*, Paris, Addison-Wesley France, 1995, p. 145.
[391] L'adresse Internet de cette société, prise au hasard parmi des centaines d'autres sur le web, est www.sequoia.be.
[392] Edelweb, www.edelweb.fr.
[393] F., LATRIVE, D., DUFRESNE, *Pirates et flics du Net*, Paris, Seuil, 2000, pp. 101 et suiv.
[394] M., CUSSON, *Croissance et décroissance du crime*, Paris, PUF, 1990, pp. 133 à 134.

Les instances internationales, et d'une certaine manière l'Etat, n'apparaissent que subsidiairement, apportant des « conseils », des indications, incitant à une nécessaire éducation, mais n'ayant pas réellement de prise sur cette matière. Nous verrons dans la partie suivante que l'Etat sera, assez logiquement, beaucoup plus présent dans le domaine de la répression.

La prévention situationnelle aura donc, outre les défauts dénoncés plus tôt, deux aspects positifs. Elle permettra de décourager les hackers les moins doués, du moins pendant un certain temps, mais surtout, elle va permettre le développement de tout un marché lié à la sécurité informatique.

En ce sens, pour reprendre l'idée de Durkheim exposée plus tôt, le crime informatique présente une certaine utilité sociale puisque, outre les progrès technologiques revendiqués par les hackers pour justifier leurs actes et la nécessaire adaptation de la loi (que nous allons aborder dans le point suivant), il devient facteur d'emplois, parfois pour les anciens pirates eux-mêmes….

Quatrième partie - Analyse de la loi du 28 novembre 2000 relative à la criminalité informatique

Stéphanie F., vingt-quatre ans, originaire de Bruges (Belgique) et jeune informaticienne : *« J'ai toujours été fascinée par les virus ; mes études d'informatique dans une grande école de Bruxelles n'ont fait que me conforter dans ma passion d'en créer »*. Rapidement repérée par des amis de la famille, elle explique : *« ils sont dans la confection et possèdent plusieurs boutiques en Belgique et en Hollande. Un jour, le fils de la famille me demande si je peux lui créer un programme qui, pour rire, irait jeter un œil dans les ordinateurs d'une des boutiques de la famille. Loin d'être compliqué, je lui écris le programme en moins de vingt-quatre heures. Je reçois, en guise de remerciement, douze mille francs belges et une superbe veste en cuir. Quinze jours plus tard, un vendredi, je revois le fils. Il m'invite chez ses parents qui souhaitent me poser quelques questions. Effectivement, les questions fusent :* « Peut-on envoyer ce fichier dans telle machine ? Est-ce que ce programme peut récupérer certains fichiers ? Peut-il être invisible ? De taille réduite ? etc. » *Mes réponses semblent être bonnes puisque le père quitte la salle pour en revenir cinq minutes plus tard. Comme dans un film, il dépose sur la table trois cent mille francs belges, soit environ sept mille six cents euros. Cet argent est à l'évidence pour moi si je peux leur créer un programme qui soit capable de voler des fichiers crées sous le logiciel Excel. Je me souviens d'avoir été plus choquée par le fait qu'ils savaient quel type de fichiers voler, et surtout chez qui, que par les billets de cinq cents et de deux milles francs belges posés sur la table. Je n'ai pas accepté. J'ai eu peur. Honnêtement, j'aurais accepté si l'entreprise avait été basée en Belgique. Mais là, la cible de ces personnes se trouve en France, dans le quartier du Sentier, à Paris. En Belgique, la législation est loin de ressembler à celle de la France »*.

Facilité, rentabilité et impunité. Voilà comment nous pourrions résumer les avantages du hacking selon cette interview réalisée par Damien Bancal[395]. A ceci prêt que pour le législateur, l'impunité pour ce type de délit est désormais à oublier en Belgique.

Il est vrai que la Belgique avait pris un certain retard par rapport aux autres pays européens et extra-européens pour adapter son arsenal législatif à la criminalité informatique. Il y eut bien une proposition de loi visant à compléter le Code pénal *en vue de réprimer les abus en matière d'informatique et l'écoute des conversations*, mais celle-ci n'a jamais passé le stade du Parlement[396].

---

[395] D., BANCAL, *Hackers et pirates sur Internet*, Strasbourg, Desmaret, 2001, pp. 32 à 33.

[396] Proposition de loi complétant le Code pénal en vue de réprimer les abus en matière d'informatique et l'écoute des conversations, *Doc. parl*., Sénat, 462-1, sess. 1988-1989, 26 octobre 1988.

Ainsi, si, dès 1973, la Suède adoptait une loi relative à la criminalité informatique, et, plus proche de nous, la France faisait de même avec la loi Godfrain du 21 juillet 1992, et les Pays-Bas avec la Wetcomputercriminaliteit du 13 mars 1993[397], il faudra attendre le 28 novembre 2000 pour voir la Belgique se doter d'une véritable loi relative à la criminalité informatique.

La loi belge de novembre 2000 poursuit deux ambitions. Elle entend tout d'abord adapter l'arsenal répressif face aux infractions liées aux nouvelles technologies. Ensuite, elle vise à résoudre les problèmes de procédure pénale inhérents à ce type de criminalité.

En conséquence, après avoir confirmé que les infractions « traditionnelles » recourant à l'informatique ne nécessitaient pas de modifier la législation existante, celle-ci étant suffisamment cohérente et complète pour les poursuivre de manière efficace[398], nous verrons que la loi introduit quatre nouvelles infractions spécifiques à l'informatique que sont le faux et l'usage de faux en informatique, la fraude informatique, le hacking et le sabotage informatique.

Etant entendu que l'analyse de la loi du 28 novembre relative à la criminalité informatique pourrait à elle seule constituer l'intégralité de notre exposé, nous nous bornerons ici à pointer les éléments déterminants, tant négatifs que positifs, induits par la loi nouvelle.

Dans le Titre I de cette partie consacrée à l'analyse des dispositions de droit pénal matériel introduites par la loi du 28 novembre relative à la criminalité informatique, nous aborderons la base légale de chaque nouvelle infraction, ainsi que l'origine et le ratio legis du texte, pour terminer par une série de commentaires.

Les mêmes remarques sont d'application pour l'analyse des adaptions apportées par la loi nouvelle à la procédure pénale belge afin de répondre aux spécificités et difficultés de la recherche et de la poursuite des infractions commises sur les réseaux informatiques, analyse qui constituera le Titre II de cette partie.

Enfin, le Titre III de cette partie sera consacrée à une analyse empirique de l'appareil policier, et en particulier de la Computer Crime Unit de Bruxelles, à l'occasion du stage que nous y avons effectué de février à avril 2000.

---

[397] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 169

[398] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 6.

Mais dans un premier temps, nous proposons de revenir sur les origines de l'élaboration de la loi du 28 novembre 2000 relative à la criminalité informatique.

Titre I – Le droit pénal matériel

Section 1 – Origine de la loi

Donnant suite à la décision du Conseil des ministres du 30 mai 1997, concernant les mesures à prendre dans le cadre de la lutte contre la criminalité informatique sur les autoroutes de l'information, l'élaboration en Belgique d'une législation en matière de criminalité informatique s'inscrit dans une double tendance.

D'une part, elle est le fruit d'une prise de conscience internationale amorcée à l'origine par l'O.C.D.E. et le Conseil de l'Europe. Les travaux de ceux-ci inciteront les états à procéder à une révision de leurs dispositions pénales en la matière, comme ce fut le cas pour la Belgique en novembre 2000[399].

Cette sensibilisation à la problématique de la criminalité informatique sera relayée par d'autres instances internationales, telles que l'Association internationale de droit pénal, le G8 ou encore l'Union européenne.

D'autre part, la loi nouvelle vise à résoudre le problème de l'inadéquation du droit pénal traditionnel à sanctionner les infractions spécifiques à la criminalité informatique, en raison notamment du caractère immatériel des données concernées[400].

Nous verrons que si ce problème ne se pose pas véritablement pour les infractions classiques perpétrées au moyen de l'informatique, les infractions spécifiques nécessitaient une interprétation évolutive de la loi.

---

[399] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 4.
[400] J.-P., SPREUTELS, « Infractions liées à l'informatique en droit belge », Rev. dr. pén., 1985, p.381.

A. LE CONTEXTE INTERNATIONAL

La prise de conscience internationale de la problématique de la criminalité informatique procède d'un mouvement assez lent ayant pris naissance dans les années quatre-vingt.

1) L'O.C.D.E.

• En 1977, l'Organisation de coopération et de développement économiques (O.C.D.E.) a commencé à chercher le moyen de garantir la protection de la vie privée et de régir les flux trans-frontaliers des données personnelles. Le conseil de l'O.C.D.E. a ainsi lancé le 23 septembre 1980 une série de recommandations à ses Etats membres, adoptées notamment par la Belgique[401].

• En 1982, l'O.C.D.E. mit sur pied un groupe de travail *ad hoc* chargé de se pencher spécifiquement sur la criminalité informatique[402].

En 1986, le rapport qui en est issu, dressé sur base d'un questionnaire adressé aux Etats membres, présente des suggestions pour l'adoption d'une politique juridique commune en matière de délinquance informatique[403]. Ce rapport se complète d'une liste d'infractions informatiques pouvant servir de modèle de base à l'élaboration d'une législation spécifique par les Etats-membres. Seront ainsi visés, en synthèse, la manipulation de données et/ou de programmes en vue de réaliser un transfert illégal de fonds ou d'autres valeurs, de commettre un faux ou d'entraver le fonctionnement d'un système informatique, la violation des droits exclusifs du détenteur d'un programme informatique et l'accès dans un système informatique sans autorisation ou l'interception d'un tel système. Enfin, le rapport visait un renforcement de la protection des secrets commerciaux et industriels.

• Par la suite, en 1995, l'O.C.D.E., par l'intermédiaire du comité PIIC (Politique de l'industrie de l'information et de la communication) mit sur pied un groupe d'experts, chargé d'analyser les questions de la sécurité, de la vie privée et de la protection de la propriété intellectuelle dans l'infrastructure mondiale de l'information[404].

Ce groupe de travail aborde différentes problématiques, comme par exemple l'usage de la cryptographie ou les codes de conduites régissant le commerce électronique. Ainsi, en octobre 2000, le comité PIIC a édité un document concernant *« la sécurité des systèmes d'informations, le présent et le futur »* dans lesquel différents points de discussion sont abordés, parmi lesquels le

---

[401] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 159

[402] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, p. 61.

[403] O.C.D.E., *La fraude informatique : analyse des politiques juridiques*, Paris, 1986.

[404] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp. 96 et suiv.

commerce électronique, le rôle respectif du secteur privé et des pouvoirs publics en matière de sécurité, les initiatives du G8, la protection de la vie privée, la culture Internet,… [405].

2) Le Conseil de l'Europe

• Le rapport dressé par l'O.C.D.E. en 1986 a servi de base aux travaux du « Comité d'experts sur la criminalité en relation avec l'ordinateur » créé au sein du Conseil de l'Europe en 1985.

Dans un premier temps, ceux-ci ont donné naissance à la « recommandation R (89)9 sur la criminalité en rapport avec l'ordinateur ». Celle-ci présente un catalogue complet d'infractions spécifiques, destiné à servir de modèle aux Etats-membres lors de la révision ou de l'élaboration d'une législation relative à la criminalité informatique[406]. Ce catalogue se présente sous la forme d'une double liste, minimale d'une part, et facultative d'autre part, selon le degré de consensus atteint au sein du Comité d'experts quant à l'évaluation du danger et de la nocivité des infractions informatiques présentées[407] :

- La *liste minimale* comprend la fraude informatique, le faux en informatique, l'effacement/endommagement de données informatiques, le sabotage informatique, l'accès non autorisé, l'interception non autorisée, la reproduction non autorisée d'un programme informatique protégé et la reproduction non autorisée d'une topographie.

- La *liste facultative* regroupe divers comportements comme l'altération de données ou programmes informatiques lorsque cette altération ne constitue pas un dommage, l'espionnage informatique impliquant la violation de secrets économiques et commerciaux, l'utilisation non autorisée d'un ordinateur ou d'un programme informatique protégé.

En tendant vers une harmonisation du droit pénal des Etats-membres en la matière, la recommandation R(89) 9 entend notamment simplifier la coopération internationale pénale, laquelle reste encore majoritairement tributaire d'exigences liées à la double incrimination[408].

---

[405] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p.96.

[406] *Recommandation R (89) 9 sur la criminalité en relation avec l'ordinateur, adoptée le 13 septembre 1989*, éd. du Conseil de l'Europe, Strasbourg, 1990.

[407] *Recommandation R (89) 9 sur la criminalité en relation avec l'ordinateur, adoptée le 13 septembre 1989*, éd. du Conseil de l'Europe, Strasbourg, 1990, p. 36 à 37.

[408] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act. dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 52.

Dans un second temps, en 1995, les travaux du Comité d'experts donneront naissance à une deuxième recommandation, dont s'est largement inspiré le législateur belge, qui aborde plus spécifiquement les questions de procédure[409].

Ces deux recommandations ont été prises en considération par le législateur belge lors de l'élaboration de l'avant-projet de loi, même si elles *« n'ont pas été suivies en tous points »*[410], notamment en raison de la relative ancienneté des textes.

- Le Conseil de l'Europe ne s'est pas arrêté en si bon chemin. En 2000, le Conseil a publié un projet de convention internationale sur la cybercriminalité[411].

Le chapitre II de cette Convention, intitulé *« mesures à prendre au niveau national »*, réserve ainsi une section au droit pénal spécial, encourageant les Etats-membres à prendre des mesures en vue d'incriminer des infractions comme l'accès illégal à tout ou partie d'un système informatique, l'interception illégale de données informatiques, la falsification informatique,….

Le projet vise également à 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.

Plus surprenant est le fait pour ce projet d'être muet sur les implications des questions de procédure pénale sur le respect de la vie privée.

La première version du projet, datant d'avril 2000, avait d'ailleurs fait l'objet de nombreuses critiques, notamment de la part des fournisseurs d'accès au réseau et des associations de défense des libertés individuelles. Les premiers dénonçaient le rôle d'auxiliaire de police que la Convention leur faisait jouer, tandis que les seconds soulevaient les risques d'intrusion dans la vie privée de chacun. Cette levée de bouclier a conduit le Conseil de l'Europe à revoir sa copie, et à rendre public une version plus allégée. Malgré tout, les opposants au projet sont toujours nombreux[412].

---

[409] *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 septembre 1995*, éd. du Conseil de l'Europe, 1996.

[410] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 9.

[411] Projet de convention du Conseil de l'Europe sur la criminalité informatique (projet N°25 REV 2), dont la dernière version est disponible sur http://conventions.coe.int.

[412] X, « La Belgique légifère en matière de cybercriminalité », *Manuel des Services de Police*, Actualités en bref n°290, 26 février 2001, p. 6.

3) L'Association internationale de droit pénal

L'Association internationale de droit pénal s'est également penchée sur la problématique de la criminalité informatique.

Dans l'esprit des recommandations de l'O.C.D.E. et du Conseil de l'Europe, ses résolutions[413] prônent des mesures de prévention non pénales, comme le développement d'une éthique de l'informatique, la promotion de la collaboration de la victime dans la dénonciation des infractions informatiques,… [414]

En ce qui concerne le droit pénal matériel, elle encourage les Etats à restreindre le champ de la répression aux seuls actes intentionnels et à incriminer les comportements énumérés dans les listes minimale et facultative.

Enfin, elle encourage les états à tenir compte de l'évolution de la technologie et des changements dans la perception de la délinquance, de manière à tenir compte d'abus ignorés par le Conseil de l'Europe, comme le trafic de mots de passe ou la distribution de virus.

Les résolutions prises par l'Association internationale de droit pénal trouveront écho auprès du Conseil de l'Europe lors de l'élaboration du projet de Convention sur la cybercriminalité qui vient d'être présenté[415].

---

[413] Voy. les recommandations du XVè congrès de l'AIDP, « section II – criminalité informatique et autres atteintes à la technologie de l'information », R.I.D.P., vol. LXVI, n°1/2, éd. Eres, Toulouse, 1995, pp. 27 et suiv.

[414] H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 166.

[415] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 53.

4) Le G8

• Le G8 s'est également intéressé au domaine de la criminalité informatique. Regroupant les 7 pays les plus riches du monde[416] ainsi que la Russie, cette structure, assez informelle et ne bénéficiant d'aucun budget particulier, se réunit chaque année pour discuter de points importants[417].

Lors du sommet de juillet 1996 en France fut créé le « groupe de Lyon », avec pour mission de s'interroger sur la sécurité dans le cyberespace, un sous-groupe étant chargé de lutter contre le crime « high tech ». Fin octobre 2000, ses membres se sont réunis à Berlin où ils se sont scindés en plusieurs ateliers réunissant des agents du secteur public, des industriels et des ONG. Trois thèmes étaient à l'étude : la localisation et l'identification des cybercriminels ; l'évaluation de la menace en matière de cybercriminalité, la prévention, la protection du commerce électronique et la confiance dans le cyberespace ; et la coopération entre les pouvoirs publics, le secteur privé et les utilisateurs[418].

• De même, lors du sommet de juillet 2000 fut adoptée la Charte d'Okinawa que voici : *« Les actions internationales pour instaurer une société mondiale de l'information doivent s'accompagner de mesures concertées pour que le cyberespace soit sûr et protégé de la criminalité. Nous devons faire en sorte que des mesures efficaces, telles qu'elles sont définies dans les lignes directrices de l'O.C.D.E. sur la sécurité des systèmes d'information, soient mises en place pour lutter contre la cybercriminalité. La coopération du G8 dans le cadre du groupe de Lyon sur la criminalité transnationale organisée sera renforcée. Nous continuerons de promouvoir le dialogue avec le secteur privé, dans le prolongement du succès de la conférence du G8 qui s'est tenue récemment à Paris intitulée : « Dialogue entre les pouvoirs publics et le secteur privé et la confiance dans le cyberespace ». Des mesures efficaces doivent être prises pour traiter les problèmes urgents liés à la sécurité, tels que le piratage et les virus. Nous continuerons à inciter le secteur privé et d'autres acteurs à protéger les vitales de l'information ».*

« Comme dans le commerce classique, où les gouvernements « font la police », l'initiative du G8 concernant la cybercriminalité veut investir les gouvernements du même rôle dans le domaine du commerce électronique. Dans ce rôle de «police », les gouvernements sont les acteurs principaux et ils comptent sur le soutien du secteur privé et autres organisations d'utilisateurs. Bien que cette mission de « police » contribue à accroître la sécurité du système en réprimant les activités délictueuses par des moyens pénaux, elle ne contribue pas directement à prévenir la perpétration de ces activités. Dans la lutte contre les délits commis

---

[416] Il s'agit du Canada, de la France , de l'Allemagne, de l'Italie, du Japon, du Royaume-Uni et des Etats-Unis.
[417] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, p.97.
[418] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp.97 et suiv.

dans le commerce classique, l'expérience montre que les efforts de prévention sont plus économiques et plus efficients que les mesures réactives que l'on doit prendre pour traiter les problèmes a posteriori, et on constate aussi que c'est le secteur privé, en coopération avec les organismes gouvernementaux compétents, qui mène la plupart de ces activités de prévention. Ces activités ne peuvent être couronnées quand elles sont spécifiquement adaptées à la branche professionnelle ou au modèle d'entreprises considérés. Les gouvernements peuvent apporter une grande contribution dans le domaine de la vulgarisation et de l'éducation et en montrant la voie, par exemple en s'assurant que les services des administrations publiques fournis électroniquement appliquent et promeuvent des normes de sécurité exigeantes »[419].

Tout comme nous l'avions mentionné plus tôt, la Charte d'Okinawa insiste sur le fait que la prévention nécessitera un effort d'éducation et d'information de la part des gouvernements.

Elle précise également le rôle important que doit jouer le secteur privé, rôle que nous avions également pointé précédemment[420].

[419] D., MARTIN, F.-P., MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, pp.97 et suiv.
[420] Voir supra la partie consacrée aux risques.

5) L'Union européenne

L'Union européenne s'est également attelée à la réglementation de la criminalité informatique.

Si, dans un premier temps, elle s'est bornée à encourager les initiatives du G8 et du Conseil de l'Europe[421], l'Union européenne a ensuite fait de la criminalité informatique une de ses priorités en publiant, à la fin du mois de janvier 2001, une Communication[422] qui, aux dires de la Commission, ne serait qu'un simple document de réflexion servant de base aux auditions et discussions habituelles. Mais il apparaît qu'elle est bien plus que cela et qu'elle constitue une synthèse précise des questions essentielles relatives à la criminalité informatique[423].

La Commission s'inscrit dans la lignée des initiatives internationales telles celles de l'O.C.D.E. et du Conseil de l'Europe.

D'une part, elle considère la nécessité d'agir sur la définition et l'incrimination de comportements illicites sur le réseau Internet, qu'il s'agisse d'infractions spécifiquement liées à l'informatique (tels le hacking par exemple), ou de délits classiques facilités ou amplifiés par les réseaux électroniques (tels la pornographie infantile, la contrefaçon ou encore le respect de la vie privée).

La communication rappelle également les directives et autres mesures communautaires adoptées et annonce la proposition d'une directive harmonisant les incriminations nationales des délits informatiques et les inscrivant dans le droit communautaire.

D'autre part, sur le plan de la procédure, la communication relève une série de questions relatives à la recherche et à la poursuite des infractions : l'interception des télécommunications, la conservation des données relatives au trafic, l'anonymat de l'accès et de l'utilisation des réseaux,… 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 la création d'un Forum Européen, rassemblant les autorités et personnes capables 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.

La spécificité de cette 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

---

[421] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 53.

[422] 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.

[423] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, p. 63.

et d'une attention constante aux problèmes de vie privée que la recherche et la poursuite des crimes informatiques sont susceptibles de poser[424].

B. LES LACUNES DE L'ARSENAL RÉPRESSIF BELGE EN MATIÈRE DE CRIMINALITÉ INFORMATIQUE SPÉCIFIQUE

Bien qu'on ne puisse parler à proprement dit de vide juridique intégral pour caractériser « l'ancien » arsenal répressif en matière de criminalité informatique[425], il nous faut néanmoins conclure à l'existence de certaines lacunes en ce domaine.

En matière de criminalité informatique non spécifique, l'application des dispositions du Code pénal ne soulève guère de problèmes, si ce n'est d'ordre procédural ; ces infractions ne différant des infractions « classiques » que par leur modus operandi[426].

La problématique naît plutôt de la confrontation des dispositions du livre II du Code pénal à la criminalité informatique, dont l'objet – des données informatiques, intangibles et incorporelles – est étranger aux prévisions et préoccupations des auteurs du Code pénal de 1867[427].

On hésite ainsi à considérer comme des *choses*, au sens de l'article 461 du Code pénal, les données informatiques frauduleusement soustraites, ou comme une *écriture*, au sens des articles 193 et suivants, les signaux numériques frauduleusement altérés,…[428]

L'application du Code pénal nécessitait donc le recours au principe de l'interprétation évolutive de la loi. Celle-ci permet aux cours et tribunaux d'adapter le sens des dispositions répressives anciennes

---

[424] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, p. 63.

[425] On peut en effet relever quelques dispositions éparses à portée limitée comme, sans prétendre à l'exhaustivité, les articles 61 à 63 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour pour la sécurité sociale, sanctionnant notamment le sabotage informatique, l'accès et le maintien illicite dans un traitement automatisé de données, et la modification ou la falsification de données informatiques. Mentionnons également les articles 259bis et 314bis du Code pénal et l'article 109ter D de la loi « Belgacom » du 21 mars 1991 portant réforme de certaines entreprises publiques économiques – tous trois consacrés à l'interception et/ou à la divulgation de télécommunications de tiers – l'article 114, § 3, de la loi « Belgacom » – qui réprime le fait de gêner ou empêcher le fonctionnement d'un réseau public de télécommunications – ou encore les alinéas 1° et 2° de l'article 114, § 8 de la même loi – sanctionnant respectivement l'usage d'un réseau de télécommunications afin de procurer, à soi ou à autrui, un avantage illicite, ainsi que le harcèlement par la voie des télécommunications.

[426] O., VANDEMEULEBROEKE, « Le droit pénal et la procédure pénale confrontés à Internet – Le droit pénal », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 170.

[427] J., PRADEL, C., FEUILLARD, « Les infractions commises au moyen de l'ordinateur », Rev. dr. pén., 1985, p. 307.

[428] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 55.

aux besoins de l'évolution technique, technologique, dans le respect de l'intention du législateur et de la lettre du texte[429].

Il en ressort que la sécurité juridique ne peut pâtir de la disparité de solutions retenues par les cours et tribunaux pour tenter de combler le vide juridique en la matière. L'affaire «BISTEL[430] » est un parfait exemple des difficultés rencontrées par la jurisprudence pour appliquer les dispositions répressives préexistantes à la criminalité informatique spécifique.

Renvoyés devant le Tribunal correctionnel de Bruxelles pour s'être introduits en fraude dans le système informatique « BISTEL » au moyen d'un modem et d'un mot de passe détourné, les prévenus étaient poursuivis du chef de faux en écriture (faux mot de passe), de vol qualifié (soustraction d'électricité), d'interception des télécommunications et de destruction de bâtiments, œuvres ou constructions (destruction du système électronique de communication). Bien qu'il prononça l'acquittement pour la quatrième prévention, au motif que le système BISTEL ne fut ni endommagé ni mis hors d'usage, le Tribunal déclara néanmoins les trois premières établies[431].

La Cour d'appel de Bruxelles réforma ce jugement, assez logiquement nous semble-t-il (en raison de l'inadaptation des incriminations utilisées), pour ne plus retenir que la prévention d'interception illicite des télécommunications[432].

Un constat similaire peut être établi pour la procédure pénale. La lourdeur des techniques d'enquêtes traditionnelles permettait difficilement de rendre compte des traces digitales laissées par les délinquants dans les systèmes informatiques.

Dans un domaine où les informations pertinentes d'un point de vue pénal peuvent, en quelques secondes, être supprimées, modifiées ou transférées à l'autre extrémité du globe grâce au réseau Internet, une adaptation du Code d'instruction criminelle aux enquêtes évoluant dans l'environnement numérique devenait indispensable.

C'est donc l'ensemble de ces éléments, internationaux et nationaux, émanant d'une prise de conscience de la problématique de la criminalité informatique, d'une part, et des lacunes de l'arsenal répressif, d'autre part, qui sont à la base de l'élaboration de la loi du 28 novembre 2000 relative à la criminalité informatique que nous allons analyser plus en détails à présent.

---

[429] *« Le juge peut appliquer la loi pénale à des faits que le législateur était dans l'impossibilité absolue de pressentir à l'époque de la promulgation de la disposition pénale, à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit certaine et que ces faits puissent être compris dans la définition légale de l'infraction »* (Cass., 15 mars 1994, *Pas.*, 1994, I, p. 261).

[430] Du nom du serveur informatique du Premier ministre (Belgian Information System by Telephone).

[431] Corr. Bruxelles, 8 novembre 1990, *Droit inform.*, 1991, n°1, pp. 51 à 56.

[432] Bruxelles, 24 juin 1991, *Rev. dr. pén.*, 1992, 340 et s.

Section 2 – Analyse de la loi

A. DROIT PÉNAL GÉNÉRAL

1) L'auteur

L'absence de précision quant à la qualité de l'auteur laisse supposer que les nouvelles dispositions sont applicables tant aux personnes physiques qu'aux personnes morales.
Ainsi, une société commerciale pourrait se voir poursuivie pour avoir accédé de manière illicite dans le système informatique d'une société concurrente pour y pratiquer de l'espionnage industriel, en vertu de l'article 550bis, §1 et §3, 1° nouveau.

2) La tentative

Pour certaines incriminations, la nouvelle loi instaure un régime particulier pour la tentative. De plus, elle érige en infraction, à part entière, certains actes préparatoires.

a) La peine applicable à la tentative

Dérogeant à l'article 53 du Code pénal, l'article 550bis, §4 nouveau, incriminant l'intrusion non autorisée dans un système informatique (le hacking), réprime la tentative d'accès de la même manière que l'infraction consommée, à savoir par un emprisonnement de 3 mois à un an et/ou une amende de vingt-six à cent mille francs.

Cette dérogation au droit pénal général ne concerne que la peine de la tentative, les éléments constitutifs de celle-ci restant régis par l'article 51 du Code pénal.

Pour le législateur, cette sévérité se justifie, d'une part, par la gravité objective du comportement incriminé, et, d'autre part, par le fait que l'auteur est souvent plus intéressé par l'obtention du code d'accès en soi que par l'accès effectif au système informatique[433].

Consécutivement à ce que nous savons désormais des hackers et de la notion de défi intellectuel motivant certaines de leurs actions, nous ne pouvons que souligner la clairvoyance du législateur sur ce point.

---

[433] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 18.

b) L'incrimination des actes préparatoires

L'article 550bis, §5 nouveau incrimine la personne qui, *avec une intention frauduleuse ou un dessein de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique, par lesquelles les infractions prévues aux §1er à 4 de l'article 550bis* (le hacking) *peuvent être commises*.

La peine prévue est un emprisonnement de six mois à trois ans et une amende de vingt-six à cent mille francs ou une de ces peines seulement.

La même peine est applicable, en vertu de l'article 550ter, §4, à celui qui, avec la même intention, *conçoit, met à disposition, diffuse ou commercialise* des données dont il sait qu'elles peuvent endommager des données ou perturber le fonctionnement d'un système informatique.

L'objet de ces incriminations, dont le champ est limité au hacking et au sabotage informatique, est de permettre la répression de la conception et de la distribution de virus informatiques et de hackertools (qui sont des logiciels permettant de violer la sécurité des systèmes informatiques).

Sans de telles dispositions, ces comportements auraient échappé à la répression, à moins de considérer que ceux-ci étaient constitutifs d'une tentative de hacking ou de sabotage.

Si cette disposition nous paraît tout à fait pertinente, c'est pour nous l'occasion de pointer l'un des manquements majeurs de la loi nouvelle. En effet, celle-ci ne définit pas les termes « données » et « système informatique », *« afin d'éviter que ces concepts soient trop rapidement dépassés par l'évolution de la technologie de l'information »*[434].

Les documents parlementaires ne donnent pas beaucoup plus d'indications précises, les « données » et les «systèmes informatiques » étant décrits par référence l'un à l'autre. Ainsi, les données sont définies comme étant *« les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique »*, et le système informatique comme *« tout système permettant le stockage, le traitement ou la transmission de données »*[435].

A titre d'exemple de systèmes informatiques, mentionnons l'ordinateur, les cartes à puces, les réseaux[436], … Selon Van Eecke, les caméras vidéos, les téléphones mobiles, le système de gestion automatique des ascenseurs,… pourront également être considérés comme des systèmes informatiques[437].

---

[434] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 12.
[435] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 12.
[436] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 12.
[437] P., VAN EECKE, « Het voorontwerp van wet inzake informaticacriminaliteit », Recente ontwikkelingen in informatica-en télécommunicatierecht, Brugge, éd. die Keure, 1999, p. 223.

3) La récidive

La loi nouvelle instaure un régime de récidive spécifique, obligatoire et temporaire pour la criminalité informatique. Ainsi, les articles 210bis, §4, 504quater, §3, 550bis, §8 et 550ter, §5 précisent qu'en cas de nouvelle infraction à ces articles dans les cinq ans du prononcé d'une condamnation du chef des infractions à ces dispositions, ainsi qu'aux articles 259bis et 314bis (relatifs aux écoutes de télécommunications), la peine est doublée.

Le juge ne disposera donc pas de la liberté d'appréciation offerte par les articles 54 et suivant du Code pénal quant à l'opportunité de majorer ou non le maximum de la peine.

Dans les autres cas de récidive, les articles 54 et suivants du Code pénal seront applicables.

4) La confiscation

Paradoxalement, alors que, comme nous l'avons vu, l'adaptation de l'arsenal répressif en matière de criminalité informatique était notamment motivé par l'impuissance du Code pénal à appréhender les atteintes aux biens incorporels que sont les données informatiques, la loi nouvelle laisse intact l'article 42 réglementant la confiscation spéciale, alors que cet article ne fait pourtant référence qu'aux notions de *« choses »* et *« d'avantages patrimoniaux »*.

Pour Meunier, cette omission risque de créer de nombreuses controverses autour de la confiscation des données informatiques immatérielles produites par l'infraction, qui en sont l'objet ou l'instrument[438].

Selon lui, cette difficulté aurait pu être éludée en complétant l'article 42 du Code pénal d'une incise visant à assimiler les données informatiques aux « choses » concernées.

5) La localisation des infractions informatiques

En l'absence de précision dans la loi nouvelle, la localisation des infractions est déterminée par référence aux principes généraux du droit pénal. Ainsi, l'infraction sera réputée avoir été commise en Belgique dès qu'un des éléments constitutifs ou aggravants aura été réalisé sur le territoire belge[439].

A l'échelle nationale, les conflits de compétence ne manqueront certainement de naître en matière de diffusion de virus par exemple, dans la mesure où la compétence devra alors s'apprécier par rapport à l'endroit où se réalise le dommage, à savoir là où se situent les ordinateurs contaminés.

---

[438] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 62.

[439] Cass. 16 mai 1989, *Pas.*, 1989, I, p. 973 ; H., BARTHOLOMEEUSEN, e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 270.

Si l'infraction présente un caractère international, ce qui est souvent le cas en matière de criminalité informatique, la compétence se résoudra en application des dispositions du titre préliminaire du Code de procédure pénale. Par souci de concision, cette matière ne sera pas abordée ici, renvoyant à la doctrine pour de plus amples informations[440].

[440] Voy ; notamment M., FRANCHIMONT, A., JACOBS, A., MASSET, *Manuel de procédure pénale*, Liège, Collection scientifique de la Faculté de droit de Liège, 1989, p. 1060 et suiv. ; F., TULKENS, M., VAN DE KERCHOVE, *Introduction au droit pénal*, Bruxelles, Story Scientia, 1998, p. 218.

B. DROIT PÉNAL SPÉCIAL

L'informatique peut constituer le but de l'infraction ou le moyen par lequel celle-ci s'opère.

C'est la distinction faite dans l'exposé des motifs de la loi de novembre 2000, preuve s'il en est que le législateur a décidé de réagir face à une criminalité informatique en constante augmentation.

L'analyse qu'il a faite de cette criminalité doit lui permettre de mieux circonscrire ses différentes composantes, et donc, de mieux la contrer. Il déclare d'ailleurs que *« force est de constater que nous somme obligés d'examiner dans le cadre de différentes branches juridiques, si les concepts juridiques classiques permettent de répondre aux nouveaux problèmes liés à la technologie de l'information »*[441].

Si cette distinction est pertinente, la terminologie utilisée nous le paraît beaucoup moins.

Prenons l'exemple du hacking. Celui-ci, comme nous le verrons dans un instant, fait partie des infractions ayant l'informatique comme but.

Ce sera clairement le cas du pirate qui s'introduit sur un site Internet afin d'en modifier le contenu.

Cependant, le hacker procédant à différentes manipulations informatiques, il serait légitime de proposer de le classer également dans la catégorie où l'informatique est un moyen de perpétrer l'infraction.

Par contre, dans le cas d'un employé de banque qui détournerait une partie des fonds sur son propre compte, le but visé est un avantage patrimonial, et non de nature « informatique », si bien que l'informatique sera ici un moyen de commettre l'infraction.

Dès lors, à la distinction de la loi du 28 novembre 2000, nous lui aurions substitué celle entre les infractions *spécifiques* à l'informatique et *aspécifiques* à l'informatique, entre celles réalisables *uniquement* grâce à l'informatique et celles *également* réalisables grâce à l'informatique.

Néanmoins, par souci de clarté, il nous a semblé plus simple d'opérer la même distinction (que celle effectuée par la loi), tout en attirant encore une fois l'attention de nos lecteurs sur les problèmes qu'elle suscite.

---

[441] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 1.

1) L'informatique comme moyen

Comme le précise l'exposé des motifs de la loi du 28 novembre 2000 relative à la criminalité informatique, la législation existante pour les infractions traditionnelles commises au moyen de l'informatique est suffisante, du moins pour incriminer et poursuivre les faits où l'informatique est un moyen de perpétration[442], étant entendu que les questions de procédure pénale (perquisitions sur des ordinateurs étrangers, saisies des données,…) seront quant à elles examinées plus tard.

Pour ce faire, nous avons choisi d'aborder brièvement deux types d'infractions où l'informatique peut constituer un moyen d'accomplissement, à savoir la pornographie infantile et les actes inspirés par le racisme ou la xénophobie.

Dans les deux cas, nous vérifierons surtout que la législation est applicable lorsque ces infractions sont perpétrées sur le réseau Internet[443], principal « nouveau » vecteur de ce type d'infractions.

a) La pornographie infantile

Il nous faut préciser que la diffusion de matériel pornographique est sanctionnée par l'article 383 du Code pénal comme outrages aux bonnes mœurs, et que c'est pour des raisons de concision que nous n'aborderons ici que la pornographie infantile.

1°) La législation existante

La Convention internationale des droits de l'enfant des Nations-Unies consacre son article 34 à la lutte contre la pornographie infantile et contre toutes les formes d'exploitation et de violences sexuelles à l'égard des enfants[444].

Cette lutte a également lieu sur le réseau Internet.

La Belgique possède 2 lois traitant de pornographie infantile.

---

[442] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , pp. 5 à 6.

[443] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , pp. 5 à 6.

[444] Convention internationale relative aux droits de l'enfant adoptée à New York le 20 novembre 1989, *M.B.* 13 juillet 1991, p. 15751 ; approuvée par la loi du 25 novembre 1991, *M.B.*,17 janvier 1992, p. 803.

Nous trouvons tout d'abord la loi du 27 mars 1995 qui insère l'article 380quinquies au Code pénal, punissant la publicité et/ou la distribution de produits pornographiques impliquant ou non des mineurs d'âge[445] :

"Article 380quinquies. - § ler. Sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de deux cents francs à deux mille francs, quiconque, quel qu'en soit le moyen, fait ou fait faire, publie, distribue ou diffuse de la publicite, de façon directe ou indirecte, même en en dissimulant la nature sous des artifices de langage, pour une offre de services à caractere sexuel ayant un but lucratif direct ou indirect, lorsque cette publicite s'adresse spécifiquement à des mineurs ou lorsqu'elle fait état de services proposés soit par des mineurs, soit par des personne prétendues telles.

La peine sera d'un emprisonnement de trois mois à trois ans et d'une amende de trois cents francs à trois mille francs lorsque la publicite visée à l'article 1er a pour objet ou pour effet, directs ou indirects, de faciliter la prostitution ou la débauche d'un mineur ou son exploitation à des fins sexuelles.

§ 2. Sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent francs à mille francs, quiconque, quel qu'en soit le moyen, fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou indirecte, même en en dissimulant la nature sous des artifices de langage, pour une offre de services à caractère sexuel ayant un but lucratif direct ou indirect, lorsque ces services sont fournis par un moyen de télécommunication.

§ 3. Dans les cas qui ne sont pas visés aux §§ ler et 2, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent francs à mille francs, quiconque aura, par un moyen quelconque de publicite, même en dissimulant la nature sous des artifices de langage, fait connaître qu'il se livre à la prostitution, qu'il facilite la prostitution d'autrui ou qu'il désire entrer en relation avec une personne se livrant à la debauche.

Sera puni des mêmes peines, quiconque, par un moyen quelconque de publicité, incitera, par l'allusion qui y est faite, à 1'exploitation de mineurs ou de majeurs à des fins sexuelles, ou utilisera une telle publicité à l'occasion d'une offre de services".

Cet article est applicable au réseau Internet.

D'une part, il est formulé de manière indépendante du point de vue technologique (*« quel qu'en soit le moyen »*).

D'autre part, le deuxième paragraphe sanctionne toute personne qui fait de la publicité pour des services à caractère sexuel fournis via un *« moyen de télécommunication ou l'autre »*. Cette disposition est donc également applicable au réseau Internet.

[445] L. du 27 mars 1995 insérant un article 380 quinquies dans le Code pénal et abrogeant l'artcile 380 quater, alinéa 2 du même Code, *M.B.* 25 avril 1995, p.10822.

Ensuite, la loi du 13 avril 1995 qui insère l'article 383bis dans le Code pénal[446] :

« Art. 383bis. § 1er. Sans préjudice de l'application des articles 379 et 380bis, quiconque aura exposé, vendu, loué, distribué ou remis des emblèmes, objets, films, photos, diapositives ou autres supports pornographique, impliquant ou présentant des mineurs âgés de moins de seize ans ou les aura, en vue du commerce ou de la moins de seize ans ou les aura, en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou fait importer, remis à un agent de transport ou de distribution, sera puni de réclusion et d'une amende de cinq cents francs à dix mille francs.

§ 2. Quiconque aura sciemment possédé les emblèmes, objets, films, photos, diapositives ou autres supports visuels visés sous le § 1er, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent francs à mille francs.

§ 3. L'infraction visée sous le § 1er, sera punie des travaux forcés de dix ans à quinze ans et d'une amende de cinq cents francs à cinquante mille francs, si elle constitue un acte de participation à l'activité principale ou accessoire d'une association, et ce, que le coupable ait ou non la qualité de dirigeant.

§ 4. La confiscation spéciale prévue à l'article 42,1 °, peut être appliquée à l'égard des infractions visées aux §§ 1er et 2, même lorsque la propriété des choses sur lesquelles elle porte n'appartient pas au condamné.

§ 5. L'article 382 est applicable aux infractions visées aux §§ 1er et 3. »

Dans cet article, les termes *« emblèmes, objets, films, photos, diapositives ou autres supports pornographique »* permettent de sanctionner la détention sur le disque dur ou sur toute autre médium électronique ou optique de matériel relevant de la pornographie infantile ; et, d'une manière générale, de prévoir les avancées technologiques en matière de stockage.

2°) La législation existante peut-elle s'appliquer au réseau Internet ?

Ces deux lois étant entrées dans l'ordre juridique interne belge, la question face à une infraction perpétrée sur le Web est celle de la loi applicable. En effet, en raison du caractère transfrontalier de celui-ci, l'infraction ou son auteur sont souvent difficiles à localiser précisément.

En droit belge, c'est le principe de territorialité qui prévaut. Ainsi, selon l'article 3 du Code pénal et une jurisprudence constante, le juge belge pourra être saisi dès que l'un des éléments constitutifs de l'infraction a été commis sur le territoire belge.

Quant à l'article 4 du Code pénal, il stipule que l'infraction commise à l'étranger par des belges ou des étrangers n'est punie en Belgique que selon les cas déterminés par la loi.

Ces cas, la loi du 13 avril 1995 les a prévus en insérant un article l0ter au Titre préliminaire du Code d'instruction criminelle. Celui-ci prévoit que le Belge ou l'étranger trouvé en Belgique qui aura commis hors du territoire une infraction à l'article 383bis du Code pénal pourra être poursuivi, et ce, même si aucune plainte ou avis officiel n'ont été reçus de l'autorité étrangère.

[446] L. du 13 avril 1995 contenant des dispositions en vue de la répression de la traite des êtres humains et de la pornographie enfantine, *M.B.*, 25 avril 1995, p. 10823.

Néanmoins, si les principes juridiques sont clairs, leur application n'est pas toujours aisée. En effet, si une infraction ne porte pas directement préjudice à quelqu'un et n'est pas soutenue par une partie civile, elle a beaucoup de chances de se voir classée sans suite.

Pour ce qui est du consommateur pornographe, il sera difficile de prouver qu'il a délibérément possédé du matériel pornographique et non qu'il soit tombé dessus « par hasard ». Si on ajoute à cela les problèmes concernant les fournisseurs d'accès qui ne vérifient par exemple pas toujours le contenu des sites qu'ils hébergent, il est aisé de comprendre la relative impunité qu'offre Internet aux pédophiles de tous les pays.

3°) Conclusions

On peut donc conclure que des lois existent, qu'elles sont applicables au réseau Internet, mais difficilement. Dès lors, il n'est pas utile, comme en convient le législateur[447], de réclamer de nouvelles lois, mais bien d'assurer les moyens nécessaires à leur effectivité (instauration d'un code éthique à suivre par les fournisseurs d'accès, aménagement de la procédure de constitution de partie civile, ...).

[447] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 6.

b) Racisme et xénophobie

Les dernières élections législatives et communales ont démontré que les partis d'extrême droite connaissaient, dans notre pays, une renaissance aussi spectaculaire qu'inquiétante. Cette résurgence apparaît comme un phénomène généralisé à tous les pays membres de la Communauté européenne, comme en témoignent les dernières élections présidentielles et législatives française de 2002.

1°) La législation existante

Les actes inspirés par le racisme ou la xénophobie sont réprimés par la loi du 30 juillet 1981, dite « Loi Moureaux »[448].

Dix ans après son entrée en vigueur, il s'avéra que 95,5 % des dossiers traités avaient donné lieu à un classement sans suite[449]. Une modification s'imposait ; ce qui fut fait, notamment, avec la loi du 12 avril 1994[450].

2°) La législation existante peut-elle s'appliquer au réseau Internet ?

Afin de répondre à cette question, nous proposons l'analyse, succincte, d'une affaire récente.

Le 22 décembre 1999, sur base de la loi du 30 juillet 1981 modifiée par la loi du 12 avril 1994, le tribunal correctionnel de Bruxelles a condamné à 6 mois d'emprisonnement avec sursis un officier de police judiciaire et ancien candidat sur les listes du Vlaams Blok à Bruxelles-Ville pour avoir tenu des propos racistes dans divers groupes de discussion[451]. Il a également été condamné à payer 100.000 FB de dommages et intérêts au Centre pour l'Egalité des Chances et la Lutte contre le Racisme, qui s'était constitué partie civile.

Avec cet arrêt, le tribunal correctionnel a démontré que notre législation actuelle était parfaitement applicable à Internet. Ainsi, en ce qui concerne

• La condition de publicité

Le tribunal considère que les newsgroups ou forums de discussion « sont *des lieux non publics mais ouverts à un certain nombre de personnes* » et qui réunissent donc la condition de

---

[448] L. du 30 juillet 1981, tendant à réprimer certains actes inspirés par le racisme et la xénophobie, *M.B.*, 8 août 1981, p. 9928.

[449] Centre pour l'égalité des chances et la lutte contre le racisme, « La loi de 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie », www.antiracisme.be/fr/, 1998.

[450] L. du 12 avril 1994, modifiant la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie, *M.B.*, 14 mai 1994, p. 12885.

[451] Corr. Bruxelles, 22 décembre 1999, *Rev. dr. étr.*, 2000, p. 121.

publicité requise par l'article 444 du code pénal[452]. En effet, selon celui-ci, la discrimination doit avoir lieu :

- soit dans des lieux publics ;
- soit dans des lieux accessibles à un nombre limité de personnes ;
- soit dans un lieu quelconque, en présence de témoins ;
- soit par des écrits faisant l'objet d'une diffusion publique ;
- soit enfin par des écrits envoyés ou communiqués à plusieurs personnes.

• La compétence territoriale

Le tribunal se déclare compétent territorialement pour connaître de l'infraction au motif que *« les faits calomnieux, la diffamation, les injures étant accomplis en tous lieux où leur diffusion est apte à être reçue ou entendue, l'imputabilité publique ayant été réalisée de cette manière; qu'en l'espèce, il est constant que la réception des messages et la participation au Newsgroup est possible en tous points du territoire belge et à fortiori dans l'arrondissement judiciaire de Bruxelles »*[453]. L'article 3 du Code pénal sera donc également d'application.

3°) Conclusions

Cet exemple nous montre très bien, en accord avec l'exposé des motifs de la loi du 28 novembre 2000 et l'ensemble de la doctrine, que la législation existante est applicable à Internet.

[452] Corr. Bruxelles, 22 décembre 1999, *Rev. dr. étr.*, 2000, p. 121.
[453] Corr. Bruxelles, 22 décembre 1999, *Rev. dr. étr.*, 2000, p. 121.

2) L'informatique comme but

En ce qui concerne les infractions ayant l'informatique comme but, nous allons voir que, tout comme pour la définition de la criminalité informatique, les classifications sont aussi nombreuses que les auteurs qui les ont réalisées.

Selon Schreiber, les infractions informatiques qui reviennent le plus fréquemment sont actuellement le piratage téléphonique, le piratage (intrusion) informatique et les programmes « malveillants » (cheval de Troie, ver, virus, …). Il base cette affirmation sur les statistiques nationales et internationales, ainsi que sur les informations officieuses et les débats qui ont lieu lors des réunions et conférences internationales[454].

Cette information est donnée à titre indicatif, étant bien entendu que le législateur se doit de définir toutes les infractions contre lesquelles il entend lutter, et non seulement les plus « populaires ».

Plusieurs possibilités se présentent lorsqu'il est question de catégoriser les infractions ayant l'informatique comme but (ou, comme nous préférions le dire, spécifiques à l'informatique).

Soit nous présentions un « florilège pratique de menaces cybercriminelles » comme l'ont par exemple fait Daniel et Frédéric-Paul Martin[455], consistant en une suite d'exemples de crimes informatiques (au sens large).

Soit nous tentions de les regrouper dans de grands groupes, à l'exemple de la classification de Grabosky, tenant compte que celui-ci ne considère pas cette liste comme exhaustive[456].

Soit nous suivions l'exemple du législateur belge qui, conscient semble-t-il de cette difficulté et nous voulant pas prendre trop de risques, s'est contenté de grouper les crimes informatiques en quatre groupes.

Cette solution nous semble la plus appropriée : un nombre trop élevé de catégories d'infractions ne sert à rien, car celles-ci présentent trop de similitudes entre elles pour être clairement distinguées.

A titre d'exemple, nous allons présenter, très succinctement, la classification de Grabosky, auteur reconnu dans le domaine de la criminalité informatique, le but étant ici de pointer ses lacunes.

---

[454] W., SCHREIBER, « La délinquance assistée par ordinateur », R.I.P.C., 1997, 51e année, n°464, pp. 9 à 10.

[455] Les auteurs étalent sur un chapitre (soit près de 50 pages) les illustrations du cybercrime (D., MARTIN, F.-P., MARTIN, *op. cit*., pp. 21 et s.).

[456] P., GRABOSKY, « Computer crime in a bordeless world », Annales internationales de criminologie, 2000, vol. XXXVIII, n°1/2, pp. 67 à 92.

Grabosky propose ainsi la classification suivante :

1) Le vol de services de télécommunications
2) Les communications servant les associations de malfaiteurs
3) Le piratage des télécommunications
4) Dissémination de documents outrageants
5) Extorsion
6) Le blanchiment d'argent électronique et l'évasion fiscale
7) Vandalisme électronique et terrorisme
8) Fraude à la vente et aux investissements
9) L'interception illégale de télécommunications
10) Fraude dans les transferts de fonds électronique

Etant bien entendu que cette classification n'a pas de portée légale proprement dite, il n'en reste que lorsque le législateur se décide à légiférer dans une matière, il va consulter différentes sources, parmi lesquelles la doctrine.

Tout d'abord, ces catégories présentent de nombreuses redondances. Ainsi, sans rentrer dans les détails que recouvrent ces différentes catégories, il nous semble que les infractions propres aux télécommunications auraient pu être placées dans une seule et même catégorie, de même que les infractions à caractère économique comme la fraude à la vente et aux investissements et la fraude dans les transferts de fonds électroniques.

Ensuite, Grabosky précisant que ces différentes formes de crimes informatiques ne sont pas mutuellement exclusives, et que dès lors, on peut par exemple voler des services de télécommunications et les utiliser à des fins de vandalisme, fraude,…, nous posons la question de l'utilité d'une telle distinction, Grabosky pointant d'ailleurs lui-même le fait que le crime informatique, comme d'autres formes de délinquance « traditionnelles », peut être mixte. Dès lors, si un vol avec violence sera compris dans l'ensemble « vol », pourquoi ne pas faire de même avec les crimes informatiques, où si les buts peuvent tout à fait différer, les techniques, de par la nécessité même de passer par l'informatique, se révèlent être généralement les mêmes ? Nous estimons que ce type de classification ne sert finalement qu'à compliquer une matière déjà très complexe, aboutissant ainsi au résultat exactement contraire à celui escompté.

L'analyse rapide de cette classification vise à montrer que s'il n'y a déjà pas d'accord au sein de la doctrine et des auteurs, la mission du législateur n'en sera que plus difficile.

Et c'est probablement devant cette difficulté que le législateur belge s'est retrouvé, choisissant de grouper les infractions en quatre grands groupes.

a) Le faux et l'usage de faux en informatique

Il existe désormais, en plus du faux en écriture « classique », un faux spécifique à l'informatique. Cette démarche tend à répondre aux problèmes posés par l'interprétation de la loi pénale.

1°) Base légale

L'article 210bis nouveau du Code pénal punit désormais d'une peine d'emprisonnement de six mois à cinq ans et/ou d'une amende de vingt-six francs à cent mille francs *« 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 techno logique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données »*.

La même peine est prévue pour *« celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses »*.

2°) Origine du texte et ratio légis

L'origine de cette incrimination spécifique est à mettre en relation directe avec l'arrêt de la cour d'appel de Bruxelles dans l'affaire BISTEL exposée plus tôt. Cette affaire avait en effet mis en lumière l'inadéquation des dispositions actuelles en matière de faux en écriture (articles 193 et suivants du Code pénal) pour incriminer la falsification de données informatiques.

La cour déclarait ainsi *« que, du moins, l'introduction, même d'une manière irrégulière, d'un mot de passe dans le système BISTEL ne constitue pas une falsification et que « le mot de passe consistant en un code électronique » utilisé par les prévenus ne constitue pas une écriture, et, plus précisément, ne constitue pas un signe graphique au sens des articles 193 et Suiv. du Code pénal ; que ne furent créés ni « faux documents », ni « fausses données » et que l'usage du faux n'est pas non plus établi »*[457].

De même, l'importance grandissante du commerce électronique, et en particulier des contrats électroniques, nécessitait la mise en place de dispositifs légaux assurant la sécurité et la fiabilité des données digitales à portée juridique[458].

---

[457] Bruxelles, 24 juin 1991, *Rev. dr. pén.*, 1992, pp. 340 et suiv.

[458] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 65.

3°) Commentaires

• Le faux en informatique ne constituant qu'une nouvelle version d'un délit « classique », nous aurions pu nous tourner vers les articles 193 et suivants du Code pénal pour incriminer ce genre de comportements, s'il n'était pas interdit d'avoir recours à une interprétation par analogie en droit pénal.

L'informatique n'entrant pas dans la définition donnée au mot « écriture » utilisée dans ces articles[459] (les données informatiques peuvent être des sons, des images, donc des éléments qui ne tombent pas sous les dispositions du faux en écriture traditionnel), les dispositions relatives au faux en écriture ne suffisaient pas pour appréhender des infractions nouvelles sur le plan technologique, comme la fabrication de fausses cartes de crédit ou encore de fausses signatures digitales. L'introduction du faux en informatique était donc indispensable.

• N'ayant pas considéré qu'une révision complète du chapitre sur le faux s'imposait, le législateur n'a pas harmonisé les dispositions relatives aux faux en informatique et le faux en écriture.

Contrairement au faux traditionnel, le faux en informatique n'établit pas de distinction quant à la nature de l'acte falsifié (acte public, authentique, commercial ou privé), ni quant à l'auteur de la falsification (fonctionnaire dans l'exercice de leur fonction ou particulier). Cet état de fait a été critiqué par le Conseil d'Etat[460], qui rappelle ce que l'exposé des motifs lui-même précise, à savoir que toute situation en ligne doit être traitée de la même manière qu'une situation similaire hors ligne[461].

Interpellé par la Conseil d'Etat, le gouvernement a justifié cette omission par la volonté de dépasser la complexité des dispositions de droit commun en matière de faux (concernant la distinction selon la nature de l'acte falsifié et selon l'auteur)[462].

Bien que les termes employés par l'article 210bis nouveau permettent d'englober aussi bien les écritures privées que les autres catégories d'écriture, il n'en reste qu'il y a bien une violation du principe d'égalité, l'auteur du faux en écritures authentiques et publiques, par exemple, étant passible d'une peine de quinze ans de réclusion, alors que la peine du faux en informatique n'excède pas cinq ans d'emprisonnement.

---

[459] Ainsi, les données informatiques peuvent, par exemple, être des sons, des images, donc des éléments qui ne tombent pas sous les dispositions du faux en écriture traditionnel.
[460] Avis du Conseil d'Etat, *Doc. parl*,. Ch. repr., 1999-2000, 0213/001 et 0214/001, p. 51
[461] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 10.
[462] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 14.

- Enfin, précisons que l'article 210bis impose que la manipulation des données informatiques par l'auteur *« modifie la portée juridique de telles données »*. Cette condition, faisant du faux en informatique une infraction *à résultat*[463], implique que l'auteur ne pourra être sanctionné que si cet objectif est effectivement atteint, ce qui sera apprécié *in concreto* par le juge de fond[464].

A défaut de résultat, la prévention retenue sera celle de la tentative de faux en informatique.

[463] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 624.
[464] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 624.

b) La fraude informatique

Lorsque l'auteur, par la manipulation de données informatiques, obtient un avantage patrimonial frauduleux en induisant sa victime en erreur, il commet une escroquerie, réprimée par l'article 496 du Code pénal.

Mais, auparavant, s'il ne leurrait non pas un être humain, mais une machine, comme un distributeur automatique de billets, la situation était toute différente. Un automate ne pouvant voir sa crédulité abusée au sens de l'article 496, le comportement du fraudeur risquait de rester impuni[465].

Ce n'est désormais plus le cas avec l'entrée en vigueur de la loi nouvelle.

1°) Base légale

L'article 504quater nouveau du Code pénal sanctionne d'une peine de six mois à cinq ans et/ou d'une amende de vingt-six francs à cent mille francs *« celui qui se procure, pour soi-même ou autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, en modifiant ou 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 ».*

2°) Origine du texte et ratio legis

Comme nous venons de l'exposer, l'apparition et le développement de mécanismes informatisés de gestion des actifs, au niveau bancaire (E-Banking, distributeurs automatiques de billets,…), industriel (transactions électroniques,..) ou autres, ont entraîné l'apparition de comportements délictueux dirigés directement contre les machines[466]. Cette particularité, associée au caractère immatériel de l'objet de l'infraction, a rapidement démontré les limites du droit pénal traditionnel à préserver l'intégrité de la propriété contre ce type d'attaques[467].

---

[465] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 627.

[466] Nous pouvons par exemple citer la technique du « salami slice », qui consiste à faire transférer, de manière automatique, sur le compte de l'auteur et à l'insu de la victime, des montants infimes mais à une fréquence élevée. Ainsi, lorsqu'une institution financière verse à ses clients une somme comportant une décimale, l'auteur arrondira ce montant à l'unité inférieure, les décimales étant détournées à son profit (ICOVE, D., *Computer crime. A crimefighter handbook*, O'Reilly & Associates, 1995, pp. 48 à 49).

[467] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 69.

Ainsi, précédemment, les seules incriminations possibles pour ce type de manipulation, à savoir le vol, l'escroquerie et l'abus de confiance, étaient inadaptées car ces infractions nécessitent la remise ou l'enlèvement matériel de l'objet visé ou une confiance trompée.

Désormais, il sera possible de punir toute une gamme d'infractions parmi lesquelles l'utilisation d'une carte de crédit volée, l'introduction d'instructions informatiques afin de modifier l'état de son compte, …

3°) Commentaires

• Certains auteurs considèrent cette définition comme étant trop large et partant, que certains actes parfaitement courants sur les réseaux informatiques pourraient désormais être qualifiés de fraude[468].

Se pose ainsi la question de l'usage des « cookies » sur l'Internet. Pour ne pas entrer dans des considérations trop techniques, nous dirons simplement qu'il s'agit d'un petit fichier texte contenant des informations relatives à la navigation de l'internaute, comme par exemple la langue dans laquelle il souhaite s'exprimer, son pseudonyme, ou encore les sites qu'il a visités.

Certains de ces cookies peuvent être directement envoyés par le site visité, le but étant, par exemple, d'enregistrer les préférences de l'internaute pour l'accueillir de la meilleure façon possible lors de sa prochaine visite. Mais ils permettront également aux entreprises de cybermarketing de connaître les centres d'intérêt de l'internaute, ses habitudes de consommation, dans la perspective d'une offre ultérieure de services.

Dès lors, les données fournies par les cookies sont susceptibles de fournir à terme, un avantage patrimonial au bénéficiaire de ces informations. Mais est-il pour autant frauduleux ?
Il nous semble que non, l'utilisation des cookies supposant l'accord implicite de l'internaute (la réception de cookies est activée par défaut dans tous les navigateurs web, mais l'internaute peut sans difficulté décider de les refuser).

Par contre, rejoignant De Villenfagne et Dussollier, nous nous posons la question de savoir si les cookies ne sont pas constitutifs d'une violation de la loi du 8 décembre 1992 relative à la protection des données à caractère personnel[469]. Ainsi, il nous semble que les informations contenues dans les cookies constituent des données personnelles au sens entendu par la dite loi, celle-ci précisant 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*

---

[468] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, pp. 66 à 68.
[469] L. du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.* 18 mars 1993, p. 5801.

éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

Enfin, à ceux qui avanceraient l'argument selon lequel tout le monde n'a pas conscience de l'existence des cookies et de leur utilisation, nous sommes tentés de leur répondre que, si « nul n'est censé ignorer la loi », nul n'est censé ignorer le fonctionnement de son ordinateur et l'utilisation qui en est faite.

- En outre, comme elle suppose un avantage patrimonial, la fraude informatique est également une infraction à résultat. Il s'ensuit que si, malgré la manipulation des données, l'auteur échoue à se faire remettre les fonds, par exemple en raison d'une défaillance du distributeur de billets, la prévention de fraude informatique ne sera pas retenue, mais plutôt la tentative de fraude[470].

- Enfin, l'exigence d'un avantage patrimonial implique qu'un étudiant s'introduisant dans le système informatique de son université pour y modifier sa cote d'examen ne pourra se voir appliquer cette prévention[471].

[470] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 628.
[471] EVRARD, S., « La loi du 28 novembre 2000 relative à criminalité informatique », J.T., 2001, p. 242.

c) L'accès non autorisé à un système informatique et les infractions voisines (le hacking)

Le hacking est certainement l'infraction nouvellement incriminée la plus importante de la loi du 28 novembre relative à la criminalité informatique.

Contrairement au faux en informatique et à la fraude informatique, le hacking (et le sabotage informatique) nécessitait une réelle adaptation du Code pénal, dans lequel on ne trouvait que des dispositions éparses mais non spécifiques à ce type d'infractions[472].

1°) Base légale

L'article 550bis nouveau du code pénal sanctionne d'un emprisonnement de trois mois à un an et/ou d'une amende de vingt-six à vingt-cinq mille francs *« celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient »*.

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.

Le paragraphe 2 du même article vise quant à lui « *celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique* ». La peine sera alors de six mois à deux ans d'emprisonnement et/ou une amende de vingt-six à vingt-cinq mille francs.

Comme nous l'avons déjà précisé, la tentative de commettre les infractions énoncées aux deux premiers alinéas est sanctionnée par les mêmes peines que l'infraction consommée[473].

La loi nouvelle fait donc une double distinction entre hacking interne (*insider*) et externe d'une part, et entre hacking externe commis avec ou sans intention frauduleuse d'autre part.

2°) Origine du texte et ratio legis

L'accès illicite aux systèmes informatiques peut, comme nous l'avons vu précédemment, se présenter sous plusieurs formes, comme la simple intrusion motivée par le jeu, le cyberterrorisme, le phreaking, …

Le hacking peut également être utilisé comme moyen de perpétration d'infractions traditionnelles, comme les harcèlements ou les menaces (grâce à un cheval de Troie par exemple).

---

[472] Cf. supra.
[473] Cf. supra.

Si l'on ajoute à ces éléments, outre la facilité avec laquelle le hacking peut être mis en oeuvre, les enseignements tirés de l'affaire BISTEL concernant l'adaptation nécessaire de la loi et la médiatisation et la généralisation de ce type de comportements, on comprend aisément la réaction du gouvernement, stimulée par le sentiment d'impunité parfois ressentie par ses auteurs[474] et inspirée des recommandations du Conseil de l'Europe présentées plus tôt (la recommandation R (89)9 et le projet de convention internationale sur la cybercriminalité).

3°) Commentaires

- Quant au hacking externe

• Comme nous l'avons déjà souligné, le concept de « système informatique » est considéré de la manière la plus large par le législateur.

Dès lors, il ressort que le champ d'application de cette disposition ne se limite pas aux systèmes informatiques pourvus de système de protection. Cette démarche s'explique par le fait qu'une telle exigence impliquerait un certain nombre de complications pratiques[475] et par le fait qu'elle se révélerait sans objet en raison de la standardisation croissante des mécanismes de protection[476].

• Pour être constatée, l'infraction ne nécessite pas qu'il y ait une dégradation du système informatique ou des données qui s'y trouvent. Le hacking est ici conçu comme un délit de mise en danger[477].

Néanmoins, la dégradation sera prise en compte au titre de circonstance aggravante (article 550bis, §3, 3° nouveau du Code pénal).

• L'article 550bis nouveau du Code pénal incrimine celui qui accède à un système sans y être autorisé, mais également celui qui s'y maintient. Bien que ces dispositions peuvent sembler redondantes (le maintien supposant un accès préalable), le législateur justifie celles-ci lorsque le hacker pénètre de bonne foi dans un système informatique, mais se rend compte, au cours de ses

---

[474] Cf. supra.
[475] Comme par exemple la nécessité de déterminer a priori les niveaux de protection requis.
[476] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 17.
[477] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 17.

déambulations informatiques, du caractère illicite de celles-ci. L'article 550bis, §1er s'appliquera si, nonobstant cette prise de conscience l'individu s'y maintient[478].

Nous nous interrogeons sur cette justification. En effet, nous ne voyons pas ce qui pourrait constituer un hacking de bonne foi, c'est à dire, d'une certaine manière, un hacking commis à l'insu de son auteur ou dont il ignorait le caractère illicite. Après avoir expliqué ce que recouvrait le concept de hacking et de hackers[479], il nous semble qu'un hacking de bonne foi est tout simplement impossible à envisager, étant entendu que tout hacking nécessite un outil technique et/ou une connaissance particulière, et partant, la perception de l'utilisation qui en sera faite.

- Ceci nous amène à parler de la controverse ayant marqué les débats relatifs à l'article 550bis nouveau, quant à l'exigence ou non d'une intention frauduleuse dans le chef du hacker.

Les sénateurs estimaient justifié d'imposer un élément moral spécifique afin d'éviter que des personnes bien intentionnées (cf. supra les Whites Hats), ayant découvert une faille dans le système de sécurité informatique d'une entreprise, ne rechignent à la rapporter, par crainte des poursuites[480]. De même, un individu s'amusant à déjouer les systèmes de sécurité, par défi ou par curiosité, sera considérée comme un criminel.

Le Conseil d'Etat soulignait à ce sujet que *« dans un contexte informatique, la simple curiosité peut susciter un délit pénal »*[481] et estime *« qu'il ne faudrait cependant pas que les adaptations du droit pénal aux progrès technologiques aboutissent à sanctionner un type de comportement alors que si ce même comportement avait été commis sans l'aide de l'informatique, il n'aurait peut-être pas donné lieu à une répression pénale »*[482].

Le législateur n'a pas suivi ces considérations, estimant que *« l'intérêt juridique protégé par les nouvelles dispositions est en premier lieu l'intégrité du système »*[483], et que ne pas punir ceux qui agiraient contre ces systèmes même sans intention frauduleuse ou dans le but de nuire *« ouvrirait la voie à toutes sortes d'abus qui mettraient danger en la sécurité des systèmes informatiques »*[484].

Malgré les critiques qu'elle suscite, cette position du gouvernement nous paraît justifiée au regard des éléments que nous avons développés dans cet exposé, notamment ceux relatifs aux motivations des hackers. Il nous semble en effet que, outre des mesures préventives comme

---

[478] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 78.
[479] Cf. supra.
[480] *Doc. parl*., Sénat, 2-392/3 – 1999/2000, p. 61.
[481] Avis du Conseil d'Etat, *Doc. parl*., Ch. repr., 1999-2000, 0213/001 et 0214/001, p. 50.
[482] Avis du Conseil d'Etat, *Doc. parl*., Ch. repr., 1999-2000, 0213/001 et 0214/001, p. 49.
[483] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 17.
[484] Justification de l'amendement n°11, *Doc. parl*., Ch repr., 0213/010, 22 septembre 2000.

l'éducation ou des mesures de prévention situationnelle[485], le seul frein possible aux infractions de hacking commises par défi ou curiosité soit une réponse pénale[486]. Nous pensons que cette incrimination permettra, peut-être, de faire prendre conscience aux hackers (et dans certains cas à leurs parents) de la gravité de leurs actes, celle-ci étant souvent proportionnelle à la peine encourue.

• Enfin, signalons que l'existence d'une intention frauduleuse ne sera néanmoins pas sans incidence, puisqu'elle constituera une circonstance aggravante.

- Quant au hacking interne

• Contrairement au hacking externe, un dol spécial est requis lors du dépassement de niveau d'autorisation accordé. Il faudra que l'auteur ait agi avec une intention frauduleuse.

Le Code pénal est donc plus exigeant quant à l'élément moral requis à l'égard de l'insider qui outrepasse son pouvoir d'accès qu'à l'égard du hacker externe, dont la seule intrusion est déjà punissable en soi.

Le législateur explique que dans le cas de l'insider, d'autres *« mécanismes moins radicaux (sanctions internes, législation du travail, droit civil, …) »*[487] doivent être abordés, le droit pénal n'étant appelé à intervenir qu'en tant qu'*ultima ratio*, pour les cas les plus graves[488].

• L'infraction suppose que l'auteur dispose d'une autorisation partielle d'accès au système informatique. Ni la loi, ni les documents parlementaires ne précisent le sens de cette autorisation partielle. Il semble néanmoins qu'elle doit être interprétée dans le sens d'une limitation « géographique », liée aux portions du système informatique librement accessible à l'utilisateur, et dans le sens d'une limitation «fonctionnelle », se rapportant aux opérations que ce dernier peut effectuer. Dans le premier cas, un employé pourrait, par exemple avoir accès à certaines parties du réseau et pas à d'autres, et dans le deuxième cas, l'utilisateur pourra effectuer certaines opérations, comme la consultation de données par exemple, sans pour autant pouvoir les modifier ou les effacer[489].

---

[485] Cf. supra.
[486] Comme pour de nombreuses infractions d'ailleurs.
[487] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 16.
[488] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 16.
[489] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 638.

- De même, il nous semble que le texte doit être étendu tant aux personnes bénéficiant d'une autorisation partielle permanente qu'aux individus dont l'habilitation est ponctuelle. Ainsi, un employé bénéficiera d'une autorisation permanente, alors qu'un consultant indépendant, appelé à effectuer des prestations déterminées, bénéficiera lui d'une autorisation limitée au temps de l'exécution de sa mission.

- Quant aux circonstances aggravantes envisagées par l'article 550bis, §3 nouveau

La peine prévue par les deux premiers paragraphes de l'article 550bis nouveau est majorée si l'auteur se trouve dans une des trois circonstances aggravantes prévues. Sera concerné l'auteur qui :

« 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, même non intentionnellement, au système 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 »

Le libellé fort général de l'alinéa 2° donne à penser que tout hacker (interne ou externe) pourrait tomber sous le coup de cette circonstance aggravante étant donné qu'il n'est pas possible, en informatique, d'accéder à un système sans l'utiliser, sans en faire *un usage quelconque*. Dès lors, les circonstances aggravantes seront systématiquement applicables et donc, les peines immanquablement alourdies.

L'exposé des motifs tempère cette conclusion en précisant que l'objet de l'incrimination est de réprimer, d'une part, la personne qui fait usage de la capacité du système attaqué, entraînant ainsi une limitation temporaire des possibilités d'autres utilisateurs (« vol de temps machine »), et, d'autre part, le hacker qui se sert d'un ou plusieurs systèmes comme relais de ses attaques, afin de brouiller les pistes, donnant l'impression que l'attaque finale provient du système intermédiaire[490].

Mais quid si le juge ne se borne pas à interpréter ce point aux objets qui viennent d'être exposés ?

La question nous paraît d'importance. En effet, si le juge ne se contente pas d'appliquer les deux premiers paragraphes de l'infraction et qu'il leur adjoint la circonstance aggravante pointée au

[490] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 17.

§3, 2°, il en résultera que le hacker *externe* (ayant agi ou non avec une intention frauduleuse) et le hacker interne (ayant agi avec une intention frauduleuse) risquent les mêmes peines, à savoir celles applicables aux actes commis avec des circonstances aggravantes, ce que le législateur voulait pourtant éviter[491].

- Quant à la provocation à commettre un hacking (article 550bis, §6)

• L'article 550bis, 6§ nouveau du Code pénal prévoit un emprisonnement de six mois à cinq ans et/ou une amende de cent francs à deux milles francs à charge de celui qui ordonne la commission d'une des infractions visées aux paragraphes 1 à 5, ou qui y incite.

La peine est donc plus lourde que celle applicable au hacker. Le législateur justifie cette pratique par la volonté de dissuader les criminels professionnels de recruter, pour l'exécution de leurs méfaits, des hackers considérant le piratage informatique comme un jeu[492].

• La disposition nouvelle ne prévoit pas que l'ordre ou l'incitation soient suivies d'effet pour être punissable.

Cette disposition nous semble dès lors parfaitement utile pour lutter contre les pratiques des groupes de hackers qui, comme nous l'avons vu avec les LoDs et les MoDs, consistent à se lancer des défis mutuels visant à s'infiltrer dans des systèmes informatiques. Dès lors, que le défi ait été ou non relevé et réussi, l'instigateur pourra être poursuivi sur base de la provocation à commettre un hacking.

Cette disposition permettra peut-être de tempérer les ardeurs de certains, le risque de se voir poursuivi étant désormais partagé par celui qui relève le défi *et* celui qui le propose.

---

[491] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, pp. 70 à 71.

[492] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 18.

d) Le sabotage

La loi envisage une gradation dans le sabotage informatique, selon le degré de gravité de ses conséquences. L'infraction principale est ainsi affectée de deux circonstances aggravantes.

1°) Base légale

L'incrimination de base, créée par l'article 550ter, § 1 nouveau du Code pénal, concerne *« 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 »*. La peine prévue est un emprisonnement de six mois à trois ans et/ou une amende de vingt-six francs à vingt-cinq mille francs.

La peine passe à un emprisonnement de six mois à cinq ans et/ou une amende de vingt-six francs à septante cinq mille francs si, suite à la commission de l'infraction précitée, *« l'auteur cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique »*.

Par contre, si l'auteur, suite à la commission de l'infraction précitée, *« empêche, totalement ou partiellement le fonctionnement correct du système informatique concerné ou de tout autre système informatique »*, la peine prévue est un emprisonnement de un an à cinq ans et/ou une amende de vingt-six francs à cent mille francs.

2°) Origine du texte et ratio legis

L'apparition et la multiplication des virus dont le seul objet est de perturber le fonctionnement des systèmes informatiques, voire de les anéantir, remettent continuellement en question la sécurité des réseaux et handicapent l'épanouissement de l'outil informatique comme instrument prioritaire de gestion professionnelle ou privée[493]. Outre les coûts importants que leur propagation implique, les virus peuvent être à l'origine de catastrophes sur le plan économique ou humain, comme dans le cas de la paralysie des réseaux informatiques de hôpitaux, des centrales électriques ou encore dans le domaine de l'aviation.

Le droit belge se devait donc de réagir, étant entendu qu'aucune disposition ne lui permettait de sanctionner la dégradation de biens immatériels. En effet, le droit pénal étant d'interprétation stricte, le Code pénal ne présentait, pour poursuivre le sabotage, que des dispositions visant la destruction, la

[493] F.-J., PANSIER, E., JEZ, *La criminalité sur l'Internet*, Paris, PUF, Coll. Que sais-je ?, 2000, p. 108.

dégradation et les dommages causés aux objets corporels[494]. Seul le cas où le virus avait détruit physiquement le système informatique pouvait se voir appliquer de telles dispositions[495].

L'article 550ter, également inspiré de la Recommandation R (89) 9 du Conseil de l'Europe, entend donc faire coïncider le droit pénal positif aux nécessités de la pratique confrontée aux nouvelles technologies.

3°) Commentaires

• Tout d'abord, précisons que la disposition nouvelle n'implique pas que les agissements de l'auteur entraînent un *dommage* aux données concernées. Ainsi, si les données introduites ne sont pas dommageables, mais entraînent simplement une action inhabituelle[496], l'auteur pourra se voir poursuivi.

Si des dommages sont constatés, il y aura lieu d'appliquer les circonstances aggravantes prévues par la disposition.

• Ceci nous amène à nous pencher sur les subtiles différences existant entre les deux types de circonstances aggravantes prévues par la loi nouvelle.

Dans le cas où la manipulation causerait des dommages, 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 »*[497].

Le législateur justifie la peine plus sévère prévue au §3 par *« l'importance que prennent les systèmes informatiques dans notre société »*[498].

• Enfin, nous rappelons que, en vertu de l'article 550ter, §4, les actes préparatoires au sabotage informatique sont sanctionnés à titre d'infraction principale.

---

[494] Voy. les articles 510 à 550 du Code pénal.
[495] Il existe des virus permettant de modifier la structure physique du disque dur. Celui-ci pouvant être comparé à une sorte de tourne-disques, le virus modifie le bras de lecture des informations sur le disque, entraînant des rayures sur celui-ci, et donc, une perte de données.
[496] Comme l'apparition d'un petit personnage sur l'écran, l'ouverture intempestive du lecteur CD-rom,…
[497] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 19.
[498] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 19.

Titre II – La procédure pénale liée à la criminalité informatique

La loi nouvelle complète son approche de la criminalité informatique par un ensemble de dispositions tendant à adapter la procédure pénale belge à l'évolution de la technique.

Le législateur a souligné qu'il n'entendait pas bouleverser le Code d'instruction criminelle[499] . Il se contente d'y introduire de nouvelles dispositions et d'adapter les textes existants aux nouvelles technologies.

Les dispositions préexistantes, inaptes à régir les recherches en milieu informatisé, contraignaient la jurisprudence à élaborer des solutions prétoriennes pour répondre aux défis de la criminalité informatique[500], parfois au prix de la sécurité juridique.

Ainsi, la recherche dans un système informatique, étant une mesure inconnue du législateur de 1808, n'était, avant l'entrée en vigueur de la loi nouvelle, pas réglementée, ce qui suscitait des hésitations quant au régime qui lui était applicable. De même, comme nous le verrons, les dispositions relatives à la saisie n'étaient à l'origine pas conçues pour être appliquées à des données informatiques. De plus, le développement des procédés de sécurisation des télécommunications digitales, comme la cryptologie par exemple, atténue l'efficacité des techniques modernes d'enquêtes comme les écoutes téléphoniques[501].

Les obstacles procéduraux se verront également multipliés par le caractère transfrontalier de la plupart des réseaux informatiques, contraignant les autorités judiciaires à recourir aux mécanismes de coopération internationale, pour la plupart lourds et formalistes[502].

---

[499] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 9

[500] D., VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet – La procédure pénale », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 243.

[501] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 95.

[502] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 96.

Section 1 – Origine de la loi

Outre le fait, comme nous venons de le préciser, de faire répondre notre arsenal procédural aux aspirations modernes de la société de l'information, la loi nouvelle entend conformer les enquêtes évoluant dans un environnement informatisé aux exigences de l'article 8 de la Convention européenne des droits de l'homme relatif au respect de la vie privée[503]. Pour ce faire, le législateur belge puise son inspiration dans les documents internationaux préexistants, parmi lesquels figure la Recommandation R (95) 13 du Conseil de l'Europe relative aux *problèmes de procédure pénale liés à la technologie de l'information*, abordée précédemment[504].

A. LES ENQUÊTES EN MILIEU INFORMATIQUE ET LE DROIT À LA VIE PRIVÉE

L'informatique est désormais partout, dans tous les domaines de la vie moderne. Tantôt outil de travail, tantôt objet de loisirs, les systèmes informatiques contiennent des données faisant partie intégrante de la vie privée de leurs utilisateurs.

Ainsi, l'analyse d'un ordinateur personnel peut révéler de nombreuses informations sur la vie privée de son utilisateur, comme son carnet d'adresses, sa correspondance privée et professionnelle, sa famille (par exemple grâce aux photographies numérisées), ses goûts en matière de musique, les sites qu'il a visités (grâce aux cookies),…., si bien que lorsque des actes d'information ou d'instruction permettent aux autorités judiciaires de prendre connaissance de ces éléments, ces actes rentrent dans le champ d'application de l'article 8 de la Convention européenne des droits de l'homme (CEDH), garantissant le droit de chacun au respect de sa vie privée.

Le premier alinéa de cette disposition étend la protection de la vie privée à la vie familiale, au domicile et à la correspondance, à laquelle sont assimilées les communications et télécommunications privées[505]. Les écoutes, qui permettent de prendre connaissance du contenu des correspondances électroniques, rentrent dès lors également dans le champ d'application de l'article 8 de la CEDH.

L'alinéa 2 de cet article autorise cependant les autorités publiques à s'immiscer dans le droit à la vie privée, à condition que l'ingérence, qui doit être prévue par la loi, soit nécessaire à la poursuite d'un des objectifs énoncés, parmi lesquels la défense de l'ordre et la prévention des infractions. La loi

---

[503] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et Protocole additionnel, signé à Paris le 20 mars 1952, approuvés par la loi du 13 mai 1955, *M.B.*,19 août 1955.

[504] *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 septembre 1995*, éd. du Conseil de l'Europe, 1996.

[505] D., VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet – La procédure pénale », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 245.

nouvelle entend répondre à cette exigence, en conférant aux enquêtes informatiques un socle légal spécifique qui leur faisait jusqu'alors défaut[506].

B. L'INSPIRATION INTERNATIONALE

Si la procédure pénale en matière de criminalité informatique a bénéficié, sur le plan international, d'une attention moins soutenue que les questions relatives au droit pénal spécial, elle a néanmoins fait l'objet de considérations détaillées de la part de l'Association Internationale de Droit Pénal (AIDP), de l'Organisation des Nations-Unies et du Conseil de l'Europe.

Les travaux de l'AIDP ont débouché sur plusieurs résolutions concernant la procédure pénale, parmi lesquelles la saisie de données intangibles, les perquisitions dans les réseaux informatiques, le devoir de coopération de tiers autres que le suspect, l'interception de communications digitales et l'emploi des preuves informatiques devant les tribunaux[507].

L'Organisation des Nations-Unies s'est distinguée avec le *« Manuel sur la prévention et le contrôle de la criminalité en relation avec l'ordinateur »*[508]. Celui-ci pointe les principaux obstacles procéduraux en matière de poursuites relatives à la criminalité informatique, et avance des solutions pour les difficultés évoquées. Le manuel traite ainsi des perquisitions sur réseau, des saisies de données digitales, de 1'obligation de collaborer dans le chefs de civils extérieurs à l'administration de la Justice, des écoutes de télécommunications digitales, de la protection des données à caractère personnel, de l'admissibilité de la preuve informatique et de la coopération internationale.

Enfin, ce sont les travaux du Conseil de l'Europe qui occupent une place de choix parmi les documents de référence en la matière.

Outre quelques réflexions esquissées dans sa Recommandation R (89) 9[509], le Conseil de l'Europe a consacré sa Recommandation R (95) 13 aux problèmes de procédure pénale liés aux technologies de l'information. Les suggestions qui y sont présentées ont été à maintes reprises traduites dans la loi nouvelle. Nous y renverrons donc au fil de l'analyse de celle-ci.

Comme nous l'avons vu précédemment, le Comité d'experts sur la criminalité dans le cyberespace du Conseil de l'Europe a rédigé un *Projet de Convention relatif à la cybercriminalité,* en

---

[506] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 98.

[507] Voy. les recommandations du XVè congrès de l'AIDP, « section II – criminalité informatique et autres atteintes à la technologie de l'information », R.I.D.P., vol. LXVI, n°1/2, éd. Eres, Toulouse, 1995, pp. 27 et suiv.

[508] « The United Nations Manuel on Computer Crime », Inter. Rev. of Crim. Pol., 1994, pp. 43-44.

[509] Voy. la *Recommandation R (89) 9 sur la criminalité en relation avec l'ordinateur et le rapport final du Comité européen pour les problèmes criminels*, éd. du Conseil de l'Europe, Strasbourg, 1990, pp. 77 et suiv..

s'inspirant des deux Recommandations précitées. Outre quelques dispositions de droit pénal matériel déjà décrites, le projet consacre deux sections à la procédure pénale[510].

Bien que controversé, ce texte constitue, selon Meunier, *« l'expression la plus avancée du consensus européen en matière de procédure pénale liée aux nouvelles technologies »*[511].

[510] Projet de convention du Conseil de l'Europe sur la criminalité informatique (projet N°25 REV 2), dont la dernière version est disponible à l'adresse http://conventions.coe.int.

[511] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 100.

Section 2 – Analyse de la loi

A. LA SAISIE DE DONNÉES INFORMATIQUES

1) Base légale

L'article 7 de la loi nouvelle insère dans le Code d'instruction criminelle un article 39bis constitué de 6 paragraphes.

Le premier précise que *« sans préjudice des dispositions spécifiques à cet article, les règles de ce Code relatives à la saisie, y compris l'article 28 sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique ».*

Les pouvoirs du procureur du Roi vis-à-vis des données informatiques pertinentes sont décrits aux § § 2 à 4, aux termes desquels :

« § 2. Lorsque le procureur du Roi découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

§ 3. Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

§ 4. Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour

empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité ».

Le § 5 ajoute que *« le procureur du Roi informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées ».*

Enfin, le § 6 veille à assurer la préservation des données après leur saisie en disposant que *« le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.*

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents ».

Enfin, signalons que l'article 10 de la loi nouvelle modifie l'article 89 du Code d'instruction criminelle, qui concerne le juge d'instruction, en rendant applicable l'article 39bis à la saisie pratiquée en cours d'instruction.

2) Ratio legis

La saisie des données informatiques – incorporelles – constituait auparavant une question problématique. En effet, les articles 35 et 39 du Code d'instruction criminelle, qui servent de base légale à la saisie, n'autorisent, outre la saisie de *« tout ce qui pourra être utile à la manifestation de la vérité »*, que la saisie des *choses* visées à l'article 42 du Code pénal, régissant la confiscation spéciale[512].

Bien que la doctrine tendait majoritairement à admettre l'assimilation des données informatiques à des *choses*[513], la question de l'application de l'article 35 du Code d'instruction criminelle à des données digitales restait controversée[514].

---

[512] Il s'agira des « choses formant l'objet de l'infraction et à celles qui ont servi ou qui ont été destinées à la commettre, quand la propriété en apparient au condamné ; aux choses qui ont été produites par l'infraction ; aux avantages patrimoniaux tirés directement de l'infraction, aux biens et valeurs qui leur ont été substitués et aux revenus de ces avantages investis ».

[513] Voy. notamment J.-P., SPREUTELS, « Le vol de données informatiques », Rev dr. pén., 1991, pp. 1050 à 1051. Celui.-ci estime que, en raison de leurs propriétés magnétique,s les données appartiennent à la réalité physique et sont donc quantifiables.

[514] Voy. D., VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet – La procédure pénale », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 261 ; P., VAN EECKE, *Criminaliteit in cyberspace*, Gand, Mys en Breesch, 1997, p. 105.

Ces difficultés étaient éludées auparavant en procédant à la saisie du support matériel contenant les données (CD, disquettes,…), mais cette mesure pouvait se révéler inutile (par exemple si les ordinateurs de la personne morale inculpée sont en réseau, sans qu'on puisse déterminer la localisation précise des données sur ce réseau) ou inopportune car disproportionnée aux besoins de l'instruction (par l'exemple lorsque la saisie porte sur l'intégralité du matériel informatique d'une personne morale, mettant ainsi sa gestion quotidienne en péril).

C'est la raison pour laquelle la loi du 28 novembre 2000 complète le Code d'instruction criminelle en y insérant un article 39bis qui permet au procureur du Roi, dans les cas où la saisie du support n'est pas souhaitable, de limiter la mesure de contrainte à la copie et au blocage des seules données pertinentes.

Ce faisant, le législateur donne ainsi corps, en droit belge, à la Recommandation R (95) 13, dont le second principe commande de *« permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie »*[515].

3) Commentaires

- Tout d'abord, il nous faut signaler que la saisie informatique entendue par la loi nouvelle est différente de la saisie répressive « classique ».

En effet, celle-ci s'entend de *« toute mesure conservatoire, prise dans le cadre d'une information ou d'une instruction, impliquant qu'un bien soit soustrait à la disposition de son propriétaire ou de son possesseur et qu'il soit mis sous le contrôle des autorités judiciaires en vue de sa production ultérieure devant les juridictions »*[516]. La saisie suppose donc la dépossession de la chose visée et le transfert de la possession aux autorités judiciaires, le but étant à la fois d'éviter la disparition des biens susceptibles de faire l'objet d'une confiscation ultérieure et d'assurer la préservation des pièces à conviction recueillies en cours d'information ou d'instruction.

Dès lors, la simple copie de données informatiques par les autorités judiciaires ne peut en soi être considérée comme une saisie pénale. Pour cela, il faudra que la copie des données soit couplée avec leur retrait du disque dur ou leur blocage, seule manière de rencontrer le critère de dépossession exigée par la saisie pénale classique. Si leur blocage ne posera pas de problème au stade de la saisie, leur destruction, selon Meunier, ne sera pas envisageable, celui-ci précisant qu'elle ne pourra intervenir qu'après leur confiscation, qui relève de la compétence du juge de fond[517].

---

[515] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 30.

[516] D., VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet – La procédure pénale », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 261.

[517] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 104.

• La saisie des données informatique doit également être distinguée de l'interception des télécommunications, car celle-ci implique le captage de données *en cours de transmission*[518].

La saisie ne s'applique qu'aux données déjà transmises ou non encore envoyées, présentes dans le système informatique.

• La copie des données pertinentes s'accompagne de la copie des données *nécessaires pour les comprendre*. Il s'agit, en d'autre termes, des clés de décryptage ou de tout autre outil de décodage des données visées (pour autant, évidemment, que celles-ci soient codées), ou encore d'un logiciel créé par l'auteur de l'infraction.

Ici aussi, la saisie de données informatiques se distingue de la saisie classique, cette situation n'étant pas prévue par l'article 35 du Code d'instruction criminelle.

• En ce qui concerne la copie des données, les alinéas 1 et 2 du § 3 pourraient paraître redondants, mais il n'en est rien. En effet, si l'alinéa 1 prévoit l'indisponibilité des « simples » données saisies, l'alinéa 2 prévoit quant à lui l'inaccessibilité des données *contraires à l'ordre public ou aux bonnes mœurs*. Si ces termes paraissent toujours redondant, il ressort des documents parlementaires que le fait de rendre inaccessibles les données nuisibles ou contraires aux bonnes mœurs doit être interprétée comme englobant *« l'élimination des fichiers concernés (c'est-à-dire leur effacement) avec conservation d'une copie pour la justice »*[519], étant entendu que d'autres mesures peuvent être prises, comme le cryptage des données.

Le paragraphe du même article 39bis précise d'ailleurs que le procureur du Roi doit communiquer au responsable du système informatique un résumé des données qui ont été copiées, rendues inaccessibles ou *retirées*.

Ce régime plus contraignant vis-à-vis des données contraires à l'ordre public et aux bonnes mœurs par rapport aux autres données informatiques (qui ne peuvent être effacées[520]) s'explique par le souci de réduire autant que possible le risque de voir ces données disséminées.

Enfin, signalons que des sites ou images pédo-pornographiques, des logiciels d'espionnage, des virus, … constituent des exemples de données contraires à l'ordre public et aux bonnes mœurs[521].

• L'article 39bis, § 5 nouveau du Code d'instruction criminelle impose au procureur du Roi

---

[518] D., VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet – La procédure pénale », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 256.

[519] *Doc. parl*., Sénat, 2-392/2, p. 11.

[520] Le paragraphe 3, alinéa 1 précise en effet que l'accès à ces données doit être empêché dans le système informatique, ce qui suppose qu'elles restent dans ce système.

[521] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, pp. 74.

« d'informer le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées ».

Cette dérogation au secret de l'information et de l'instruction se justifie par un souci de transparence vis-à-vis de la personne – physique ou morale – intéressée, pour les activités de laquelle les informations recueillies une importance capitale[522]. Elle lui permet en outre d'évaluer en connaissance de cause l'opportunité de demander la mainlevée de la saisie dan le cadre du référé pénal.

Celui-ci est en effet rendu applicable à la saisie de données informatiques par l'article 39bis, 6, § 1 en renvoyant à l'article 28sexies du Code d'instruction criminelle. Ainsi, toute personne lésée par une saisie ou un blocage de données peut en demander la mainlevée au procureur du Roi.

Cette incise vise à répondre à l'invitation faite par la Recommandation R (95) 13 du Conseil de l'Europe de rendre applicable, à la saisie de données informatiques, les recours juridiques prévues par la législation interne en matière de saisie[523].

---

[522] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 21.

[523] Voy. Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 30.

B. L'EXTENSION DE LA RECHERCHE DANS UN MILIEU INFORMATIQUE

1) Base légale

La recherche dans un milieu informatique est réglementée par l'article 88ter nouveau du Code d'instruction criminelle.

En son paragraphe 1er, cette disposition précise *que « lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, 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 ».

Le paragraphe 2 ajoute, quant aux limites « géographiques » de la recherche, que celle-ci *« ne peut pas excéder 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 ».*

Dans l'hypothèse où la recherche se complète d'une saisie de données informatiques, le paragraphe 3 dispose qu'en *« ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39bis s'appliquent. Le juge d'instruction en informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées ».*

L'alinéa 2 du même paragraphe décrit les pouvoirs du juge d'instruction vis-à-vis de données situées à l'étranger en ces termes : *« lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la justice, qui en informe les autorités compétentes de 1'état concerné, si celui-ci peut raisonnablement être déterminé ».*

Enfin, le paragraphe 4 rend l'article 89bis du Code d'instruction criminelle, concernant la délégation en matière de perquisition, applicable à l'extension de la recherche dans un système informatique.

2) Ratio legis

Comme la visite domiciliaire, la recherche informatique est soumise à des conditions et limitations tenant tant aux heures auxquelles elle est admise, qu'à la localisation précise du système informatique visité.

Avant l'entrée en vigueur de la loi nouvelle, lorsque les enquêteurs constataient, au cours de leurs recherches, que des données pertinentes étaient logées dans un segment du réseau situé en un autre lieu que celui mentionné dans le mandat, ils se trouvaient dans l'incapacité de s'y rendre, ne serait-ce que virtuellement, en parcourant le réseau informatique[524]. Un nouveau mandat de perquisition devait alors être délivré.

On peut se poser la question de savoir comment, avant l'entrée en vigueur de la loi nouvelle, le juge d'instruction était censé déterminer la localisation précise d'informations, au moment de rédiger le premier mandant, alors que celle-ci n'apparaîtra souvent qu'au cours de la recherche elle-même.

De plus, la volatilité caractéristique des données informatiques fait courir le risque de voir celles-ci disparaître ou déplacées entre le moment de l'alerte consécutive à la première perquisition et la délivrance du second mandat. Pour éviter cette disparition, le juge d'instruction procédait à l'exécution de perquisitions simultanées en plusieurs endroits. Mais cette option, outre sa difficulté sur le plan logistique, supposait que le magistrat soit préalablement au courant des diverses ramifications du réseau et de leur situation géographique, ce qui n'est pas nécessairement le cas.

Toutes ces carences justifiaient une adaptation de la procédure pénale aux spécificités du réseau. Cette adaptation de la matière relative aux perquisitions en droit belge répond ainsi également aux souhaits de la Recommandation R(95) 13 du Conseil de l'Europe de conférer aux enquêteurs le pouvoir d'étendre la perquisition à d'autres systèmes informatiques qui sont connectés par le biais d'un réseau et d'y saisir des données, à condition qu'une action immédiate soit requise[525].

Signalons enfin que le projet de Convention sur la cybercriminalité du Conseil de l'Europe contient également un article relatif à cette matière. Celui-ci, en son article 19.2 précise que *« chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, en recourant aux mesures visées au § 1, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, sur son territoire ou en un autre lieu relevant de sa souveraineté, et que ces données sont légalement accessibles à partir du système initial ou*

---

[524] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 35.

[525] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 35

disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un moyen d'accès similaire à l'autre système »[526].

3) Commentaires

• Assez paradoxalement, la loi nouvelle, si elle définit les conditions d'extension de la recherche, ne précise par contre pas le statut de cette recherche.

Plusieurs auteurs la considèrent comme une forme de perquisition[527]. Comme le domicile, l'ordinateur peut être considéré comme un lieu d'exercice de l'activité privée et professionnelle d'une personne[528].

Dès lors, il semble légitime d'étendre *« au domicile informatique »*[529] que constitue l'ordinateur, le statut d'inviolabilité octroyé au domicile par la Constitution et les conventions internationales, et d'y appliquer les dispositions relatives à la perquisition[530].

• Si la recherche en milieu informatique est assimilée à la perquisition, la compétence pour ordonner cette mesure revient en principe au juge d'instruction. Dès lors, il en ira de même pour l'extension de la recherche dans le système informatique (ce que confirme l'article 88ter qui ne mentionne que le juge d'instruction).

Le procureur du Roi ne sera ainsi habilité à procéder à une recherche dans un système informatique privé qu'en cas de flagrant délit (article 3§ du Code d'instruction criminelle) ou moyennant le consentement de la personne ayant la jouissance effective du système informatique. Comme l'extension de la recherche se voit appliquer les mêmes conditions que la recherche en milieu informatique, et donc, de la perquisition, il en résulte qu'en cas de recherche effectuée avec le consentement du gestionnaires du système informatique, si celle-ci s'étend au-delà de ce système, le gestionnaire du système touché par l'extension devra également donner son consentement.

---

[526] Projet de convention du Conseil de l'Europe sur la criminalité informatique (projet N°25 REV 2), dont la dernière version est disponible à l'adresse http://conventions.coe.int.

[527] D., VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet – La procédure pénale », in *Internet sous le regard du droit*, Bruxelles, Editions du jeune barreau de Bruxelles, 1997, p. 256 ; P., VAN EECKE, *Criminaliteit in cyberspace*, Gand, Mys en Breesch, 1997, p. 105 ; C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 663.

[528] H.D., BOSLY, D., VANDERMEERSCH, *Droit de la procédure pénale*, Brugge, La Charte, 1999, p. 308.

[529] *Rapport explicatif de la Recommandation R(89) 9 du Conseil de l'Europe*, éd. du Conseil de l'Europe, Strasbourg, 1990, p. 56.

[530] Il s'agit des articles 32, 36, 87 et 88 du Code d'instruction criminelle, ainsi que la loi du 7 juin 1969 fixant le temps pendant lequel il peut être procédé à des perquisitions ou à des visites domiciliaires.

• La compétence territoriale du magistrat répond aux critères « classiques » exposés par l'article 62bis, alinéa 1 du Code d'instruction criminelle.

L'extension de la recherche dans un autre arrondissement est couverte par les articles 23, alinéa 2, et 62bis, alinéa 2, du Code d'instruction criminelle. Ceux-ci autorisent le procureur du Roi et le juge d'instruction à faire procéder, en dehors de leur arrondissement, à tous les actes de police judiciaire, d'information et d'instruction relevant de leurs attributions, à condition d'en avertir le procureur du Roi de l'arrondissement dans lequel l'acte doit être accompli.

Bien qu'il ne s'agira ici que d'un déplacement virtuel et non physique, la doctrine estime que cette exigence de notification doit être maintenue, dans le souci d'une coordination correcte de l'action publique au niveau national[531].

• L'extension de la recherche est subordonnée à trois conditions.

La première, obligatoire, veut que l'extension de la recherche soit *nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche*. Le législateur justifie cette exigence restrictive en raison du caractère exceptionnel de l'extension de la recherche informatique[532]. Il se déduit de cette expression que l'extension de la recherche ne sera admise que pour des données permettant d'apporter des éléments à charge et/ou à décharge[533]. Ce sera au juge d'instruction d'apprécier, *in concreto*, si l'extension de la recherche est nécessaire ou non[534].

De plus, la nécessité requise ne s'impose qu'à *« l'égard de l'infraction qui fait l'objet de la recherche »*. Il en résulte que le juge d'instruction ne pourra étendre la recherche à des données pouvant servir de preuves à des faits dont il n'est pas saisi. Par contre, si dans le cadre de la recherche informatique, il prend connaissance d'un flagrant délit, il pourra se saisir d'office et ordonner une extension de la recherche pour ces nouveaux faits[535].

Les deuxième et troisième conditions sont alternatives : il faudra soit, que d'autres mesures soient disproportionnées, soit qu'il y ait un risque que des éléments de preuve soient perdus sans cette extension.

---

[531] B., DEJEMEPPE,, « Les lignes directrices de la réforme de l'information pénale », in *La loi du 12 mars 1998 réformant la procédure pénale*, CUP, éd. Collection Scientifique de la Faculté de Droit de Liège, 1998, p. 65. C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 666.

[532] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 23.

[533] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 666.

[534] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. 45, février 2000, p. 122.

[535] M., FRANCHIMONT, A., JACOBS, A., MASSET, *Manuel de procédure pénale*, Liège, Collection scientifique de la Faculté de Droit de Liège, 1989, p. 297.

L'exigence de proportionnalité sera par exemple remplie lorsque le juge, recherchant une donnée précise, recoura à l'extension de la recherche plutôt que de délivrer autant de mandats qu'il y a de filiales de la personne morale inculpée[536].

La deuxième condition sera probablement plus fréquemment invoquée. Si les enquêteurs doivent attendre la délivrance d'un nouveau mandat de perquisition pour accéder à la partie du système renfermant les données jugées pertinentes, ils risquent, entre-temps, de voir l'auteur détruire et ou modifier lesdites données.

Si ces conditions ne sont pas remplies, les enquêteurs, pour accéder aux données recherchées situées en un autre lieu, devront obtenir un nouveau mandant de perquisition.

- Pour terminer, nous allons abordés quelques points relatifs aux limites de l'extension de la recherche informatique.

Tout d'abord, l'article 88ter, § 2 nouveau interdit au juge d'instruction, dans le cadre de l'extension de la recherche d' « *excéder 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'objet de cette restriction spatiale est d'empêcher que l'extension ne soit illimitée et ne touche l'ensemble des systèmes susceptibles d'être en relation ou d'être mis en relation avec le système informatique[537].

A ce sujet, nous posons la question de savoir si le juge d'instruction pourra étendre la recherche dans un ordinateur portable ponctuellement connecté au système perquisitionné. Selon l'exposé des motifs, il semblerait que non, la liaison technique devant présenter un élément de *permanence* et de *stabilité* et ne pouvant être purement *occasionnelle*.

A notre sens, si le juge d'instruction estime, *in concreto*, que l'ordinateur portable peut contenir des données *nécessaires à la manifestation de la vérité* et que de *éléments de preuve risquent d'être perdus*, l'extension de la recherche devrait être autorisée.

Cette disposition interdit également de facto aux enquêteurs de procéder au hacking du système informatique visé[538], en l'infiltrant à partir de leurs propres ordinateurs par exemple. Une telle pratique, qu'elle ait lieu sur le système visé ou à partir d'un autre ordinateur, serait illégale, se réalisant

---

[536] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. 45, février 2000, p. 124.

[537] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 23.

[538] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 23.

à l'insu du gestionnaire du système et excédant l'autorisation d'accès des utilisateurs habilités (les enquêteurs pourraient donc être poursuivis en vertu de l'article 550bis exposé supra).

De plus, cette pratique ne répondrait pas aux principes de légalité et de loyauté de la preuve[539], dont le juge d'instruction est le gardien en vertu de l'article 56, § 1er du Code d'instruction criminelle[540].

Ensuite, se pose la question de l'extension de la recherche dans le cas où celle-ci devrait dépasser nos frontières.

Si les données se trouvent sur le territoire national, l'article 88ter, § 3, alinéa 1 nouveau rend applicables les règles prévues à l'articles 39bis, auquel, dès lors, nous nous permettons de renvoyer.

Par contre, *« lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la justice, qui en informe les autorités compétentes de 1'état concerné, si celui-ci peut raisonnablement être déterminé ».*

Par cette disposition, la loi nouvelle autorise le juge d'instruction à poser un acte de contrainte, supposant déjà un acte attentatoire à la vie privée (puisque la copie des données suppose que le juge d'instruction en ait préalablement pris connaissance), risquant ainsi de porter atteinte à la souveraineté de l'Etat concerné par l'extension de la recherche informatique.

Cette disposition est motivée par des considérations pragmatiques. En raison de l'extension internationale des réseaux informatiques et de la difficulté de localiser *a priori* les données recherchées, il est possible que, dans le cadre d'une recherche informatique, les autorités judiciaires prennent connaissance de fichiers avant de se rendre compte que ceux-ci se trouvent à l'étranger[541].

Selon l'exposé des motifs, les preuves ainsi recueillies devraient être admises s'il apparaît que les autorités judiciaires ignoraient que les données informatiques se trouvaient à l'étranger. Il précise encore que recourir aux mécanismes traditionnels de la coopération internationale, lourds et formalistes, risquerait d'aboutir à la perte des données informatiques recherchées[542], .

Compte tenu du risque de violation de la souveraineté d'états tiers, il est précisé que la mesure ne pourra constituer qu'en une copie des données et qu'elle ne sera permise que si l'élément d'extranéité n'apparaît pas *a priori*[543].

---

[539] Voy. M., FRANCHIMONT, A., JACOBS, A., MASSET, *Manuel de procédure pénale*, Liège, Collection scientifique de la Faculté de Droit de Liège, 1989, p. 757 et suiv.

[540] H.D., BOSLY, I., WATTIER, « L'instruction », in *La loi du 12 mars 1998 réformant la procédure pénale*, CUP, éd. Collection scientifique de la Faculté de Droit de Liège, 1998, p. 134.

[541] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 23.

[542] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 24

[543] Projet de la loi relatif à la criminalité informatique,*Doc. parl*., Sénat, 2-392/3, p. 78.

Cette disposition fut sévèrement critiquée, par le Conseil d'Etat et la doctrine, au motif que, en l'absence de tout traité international autorisant les autorités belges à empiéter, ne serait-ce que virtuellement, sur le territoire d'un autre Etat, la loi belge ne peut établir unilatéralement un mode particulier de coopération entre états[544]. D'ailleurs, la Recommandation R(95) 13 du Conseil de l'Europe précise en ce qui concerne l'extension de la recherche informatique : *« il convient également de respecter les limitations imposées par le droit international. Dès que les autorités chargées de l'enquête d'un état membre disposent d'éléments indiquant qu'une perquisition sur réseau a dépasser leur pouvoir de perquisition, celle-ci n'est probablement plus valable. Dans des cas pareils, la perquisition doit être interrompue si ce type d'investigation ne fait pas l'objet d'un accord bilatéral ou multilatéral avec l'état concerné »*[545].

Il est à noter que l'article 32 du projet de Convention sur la cybercriminalité du Conseil de l'Europe prévoit la possibilité pour les parties contractantes de procéder à de telles recherches informatiques[546].

En outre, l'utilisation de cette possibilité par les autorités judiciaires belges risque d'entraîner l'irrégularité de la preuve si les données recueillies font l'objet, à l'étranger, d'une protection particulière, par exemple au titre de données à caractère personnel[547].

Selon Meunier, la situation sera différente si, préalablement à la copie des données situés à l'étranger, les autorités judiciaires ont obtenu l'accord exprès du gestionnaire du système concerné, étant entendu qu'il ne s'agira donc plus d'un acte de contrainte[548].

---

[544] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act.dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. 45, février 2000, p. 129.

[545] *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 septembre 1995*, éd. du Conseil de l'Europe, 1996, p. 38.

[546] Projet de convention du Conseil de l'Europe sur la criminalité informatique (projet N°25 REV 2), dont la dernière version est disponible à l'adresse http://conventions.coe.int.

[547] Avis du Conseil d'Etat, *Doc. parl*., Ch. repr., 0213/001, p. 48.

[548] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 678.

C. LA COOPÉRATION DE TIERS

1) Base légale

L'obligation faite aux tiers de collaborer à l'enquête en milieu informatisé trouve sa base légale dans les articles 88quater d'une part, et 90quater, § 4, d'autre part.

En vertu de l'article 88quater, § 1er nouveau *« 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 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. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi ».*

Le paragraphe 2 ajoute que *« 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 ».*

Selon l'alinéa 2 du même paragraphe *« l'ordonnance visée à l'alinéa 1er ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156 ».*

La loi nouvelle complète l'article 90quater, relatif aux écoutes téléphoniques d'un paragraphe 4, disposant que *« le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les 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'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.*
Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens ».

En vertu du paragraphe 5, *« l'État est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système ».*

Pour les deux dispositions, si la personne concernée refuse de fournir la collaboration ordonnée, celle-ci est punie d'un emprisonnement de six mois à un an et/ou une amende de vingt-six francs à vingt-six francs (article 88quater, § 3 et 90quater, § 4, alinéa 3). Il en va de même, en ce qui concerne l'article 88quater, de celui qui fait obstacle à la recherche dans le système informatique.

Enfin, les deux dispositions imposent à la personne dont la collaboration a été requise de garder le secret, à peine de se voir sanctionner conformément à l'article 458 du Code pénal (articles 88quater, § 4 et 90quater, alinéa 4).

2) Ratio legis

La menace croissante que constitue la criminalité informatique pour l'intégrité des systèmes informatiques oblige de plus en plus fréquemment les utilisateurs et les gestionnaires à pourvoir leurs systèmes de systèmes de sécurité. Comme nous l'avons vu, ces dispositifs peuvent prendre la forme de codes d'accès, du recours à des techniques de chiffrement de données ou encore au cryptage des télécommunications. Si cette mesure peuvent avoir une utilité certaine (à condition, comme nous l'avons déjà précisé, de les utiliser correctement et de les coupler avec une bonne information de leurs utilisateurs), elles peuvent également constituer un obstacle à l'action des autorités judiciaires, dans la mesure où elles restreignent la possibilité d'accéder au système informatique concerné ou de prendre connaissance du contenu des télécommunications interceptées[549].

De plus, le Code d'instruction criminelle ne contenait pas, jusqu'à présent, de disposition permettant au juge d'instruction ou au procureur du Roi à requérir, sous la menace d'une sanction pénale, l'aide technique d'un spécialiste du système informatique ou de télécommunications visé par les investigations[550].

La loi nouvelle entend répondre à cette lacune, donnant ainsi corps, en droit belge, à la Recommandation R (95) 13 du Conseil de l'Europe[551].

---

[549] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 56.

[550] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 26.

[551] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 56 et 61.

3) Commentaires

- Quant à la nature de la collaboration

La collaboration contrainte de tiers ne constitue ni un témoignage[552], ni une expertise[553]. Elle doit plutôt être assimilée à une réquisition, permettant aux autorités judiciaires de contraindre une personne étrangère à l'administration de la justice à leur prêter assistance dans l'exercice de leur mission[554]. Un autre exemple de réquisition peut être trouvé dans les dispositions du Code d'instruction criminelle relatives à l'écoute et au repérage de télécommunications (articles 88bis et 90ter et suivants), en vertu desquelles le juge d'instruction peut imposer aux opérateurs de réseaux de télécommunication et aux fournisseurs de services de télécommunication une obligation spécifique de collaboration[555].

- Quant à la compétence

C'est au juge d'instruction que revient la compétence de principe de prendre cette mesure.

Mais, bien que le texte ne prévoie pas expressément, il semble logique de reconnaître la même compétence au procureur du Roi en cas de flagrant délit ou sur consentement, à peine de priver d'efficacité les perquisitions dans le système informatique ou l'interception des télécommunications qu'il peut ordonner dans ces circonstances[556].

- Quant aux modalités de l'obligation de coopération

Selon l'article 88quater, le juge d'instruction peut imposer deux types d'obligations, à savoir, d'une part, une obligation d'information, et, d'autre part, une obligation d'intervention.

---

[552] Le tiers requis n'est pas appelé à rapporter à la justice ce qu'il a observé des faits délictueux (voy. M., FRANCHIMONT, A., JACOBS, A., MASSET, *Manuel de procédure pénale*, Liège, Collection scientifique de la Faculté de Droit de Liège, 1989, p. 331)

[553] Le tiers n'est pas appelé à fournir au juge des éclaircissement sur des aspects techniques qui le dépassant (voy. M., FRANCHIMONT, A., JACOBS, A., MASSET, *Manuel de procédure pénale*, Liège, Collection scientifique de la Faculté de Droit de Liège, 1989, p. 331).

[554] Voy. ainsi l'article 42, alinéa 1, de la loi du 5 août 1992 sur la fonction de police, qui précise que *« lorsqu'il est mis en danger dans l'exercice de sa mission ou lorsque des personnes sont en danger, tout fonctionnaire de police peut requérir l'aide ou l'assistance des personnes présentes sur place. En cas d'absolue nécessité, il peut même requérir l'aide ou l'assistance d toute autre personne utile » (*L. du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992, p. 27124).

[555] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 681.

[556] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 682.

Le paragraphe 4 du même article le précise que les personnes qui ont connaissance de la mesure ou y prêtent leur concours sont tenues de garder le secret, sous peine d'être sanctionnées conformément à l'article 458 du Code pénal.

- L'obligation d'information

Selon le paragraphe 1er de l'article 88quater, le juge d'instruction peut d'imposer aux tiers requis de *« fournir des informations sur le fonctionnement du système informatique 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 »*.

Il pourra ainsi demander au fournisseur du matériel de lui en préciser les spécificités techniques, au gestionnaire du réseau de lui communiquer le code d'accès, de lui fournir des précisions sur le réseau interne de l'entreprise ou encore demander les clés de cryptage permettant de décoder les données protégées[557].

Les personnes concernées par cette obligation d'information sont celles dont le juge d'instruction *« 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 »*. Le texte est libellé en des termes extrêmement larges, laissant ainsi au juge d'instruction une grande marge d'appréciation quant à la personne à laquelle il convient de faire appel[558], ce choix se faisant au cas par cas[559].

Il s'agira ainsi des importateurs ou distributeurs d'ordinateurs ou de logiciels, des *« trusted third parties »* (« tiers de confiance »)[560], des fournisseurs de service, des ingénieurs d'entreprise, des spécialistes de la sécurité, des informaticiens indépendants, …[561]

- L'obligation d'intervention

Selon l'article 88 quater, § 2, le juge d'instruction peut obliger la tierce personne requise à *« mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher,*

---

[557] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 27.

[558] En l'absence de précision de la part du législateur, il semble qu'il puisse s'agir tant d'une personne interne qu'externe à l'entreprise.

[559] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 27.

[560] Il s'agit de la personne ou de l'organisme institué dépositaire des clés privées d'utilisateurs de programmes de chiffrement (voy. BECKER, N., « La cryptographie et la confidentialité des données : une question clé… », Rev. Ubiquité, 1998, p. 62).

rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système ». Cette énonciation englobe toutes les manipulations que la loi nouvelle permet aux autorités judiciaires d'effectuer sur les données ou les systèmes.

Il est également précisé que l'obligation de la personne requise est une obligation de moyen. Elle ne pourra donc pas être sanctionnée si elle échoue en raison de son incompétence.

L'article 88quater nouveau prévoit que le juge d'instruction peut imposer cette obligation d'intervention *« à toute personne appropriée »*. Il s'agit des personnes capables d'exécuter, d'elles-mêmes ou sur ordre du juge d'instruction, les opérations énoncées par le texte[562]. Il peut s'agir de l'utilisateur habituel de la machine, d'un informaticien indépendant ou interne à l'entreprise, d'un responsable de la sécurité du réseau, ... le juge appréciera, ici aussi, au cas par cas.

Le texte n'impose pas que cette intervention ait lieu en présence des autorités judiciaires.

Certaines catégories de personnes sont exemptées du devoir de collaborer.

Ainsi, conformément au paragraphe 2, alinéa 2, l'inculpé et ses proches dérogent à cette obligation.

Le législateur évite ainsi l'écueil fréquent dans les lois pénales informatiques qui imposent à l'accusé de collaborer au décryptage ou au déverrouillage des données saisies ou communiquées[563]. C'est notamment le cas dans la loi néerlandaise que l'Ordre National des Avocats a sévèrement critiquée sur ce point[564]. 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[565], lui-même découlant du principe de la présomption d'innocence garantie par l'article 6.1 de la Convention européenne des droits de l'homme. Cette protection bénéficie également, en vertu de l'article 61 bis du Code d'instruction criminelle, à toute personne à l'égard de laquelle l'action publique est engagée dans le cadre de l'instruction, et qui bénéficie des mêmes droits que l'inculpé.

Les proches de l'inculpé dérogent également à cette obligation afin d'éviter de les voir forcés de rassembler des éléments de preuves contre un membre de leur famille sous la contrainte de

---

[561] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 27.

[562] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 27.

[563] F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, pp. 76.

[564] Th., DE ROOS, « Het concept-wetsvoorstel computercriminaliteit II », Computerr., 1998/2, p. 57.

[565] Cour eur.D.H., arrêt (SAUNDERS c. Royaume-Uni) du 17 décembre 1996, *J.D.F.*, 1997, pp. 98 ;Voir. KUTTY ; F., « L'étendue du droit au silence en procédure pénale », Rev.dr. pén., mars 2000, pp. 330 à 331.

sanctions pénales. Néanmoins, le recours aux proches est possible lorsque l'inculpé ne s'y oppose pas, conformément à l'article 156 du Code d'instruction criminelle.

En outre, dès qu'un doute existe dans l'esprit du juge d'instruction quant à l'implication éventuelle d'une personne non encore inculpée, on conçoit que le magistrat s'abstienne de requérir son assistance active, à peine de ruiner les poursuites si cette personne devait se voir ultérieurement inculpée. Ce genre d'hésitation peut par exemple survenir lorsque le juge d'instruction désire faire appel à un spécialiste employé par la personne morale inculpée.

Enfin, bien que le texte de loi ne le précise pas, les personnes dépositaires du secret professionnel, en vertu de l'article 458 du Code pénal, ne peuvent être tenues de coopérer à l'instruction sur la base de l'article 88quater nouveau du Code d'instruction criminelle.

Selon le législateur, ces personnes sont soumises au même régime que si elles étaient appelées à témoigner en justice[566] : elles peuvent collaborer à la recherche sans cependant y être contraintes[567].

Il précise également que *« le but n'est pas de déroger au droit commun en matière de secret professionnel »*[568].

Cette attitude, en accord avec la doctrine[569], nous semble assez pertinente, à peine de vider l'obligation au secret de son contenu, si son dépositaire était tenu de collaborer.

- Quant à la responsabilité pénale de l'Etat

L'article 88quater, § 5 nouveau rend l'Etat *« civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système »*.

Cette disposition est assez logique car il serait injuste de rendre ces personnes responsables du dommage causé, alors que leur intervention leur a été imposée sous la menace d'une sanction pénale. Il en va bien entendu différemment si le dommage a été occasionné intentionnellement par la personne requise[570].

---

[566] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 28.
[567] H.D., BOSLY, D., VANDERMEERSCH, *Droit de la procédure pénale*, Brugge, La Charte, 1999, p. 391.
[568] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 28.
[569] Voy. 682.
[570] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 27.

- Quant l'article 90quater, §4 nouveau du Code d'instruction criminelle

Cet article, qui est le pendant de l'article 88quater en matière d'écoute de télécommunications, permet également au juge d'instruction d'imposer une obligation d'information ou d'intervention à des tiers. Le but de cette disposition est de remédier aux obstacles que dressent, pour la prise connaissance du contenu des télécommunications digitales, les procédés de cryptage.

Le régime de l'article 90quater étant similaire à celui de l'article 88quater, nous y renvoyons pour l'essentiel. Néanmoins, il existe principalement deux différences avec celui-ci.
Tout d'abord, les personnes concernées sont celles dont *« le juge d'instruction présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de crypter les données qui sont stockées, traitées ou transmises par un système informatique »*.

Cette obligation à donc une portée plus large que le paragraphe 2 du même article 90quater, imposant aux seuls opérateurs de réseaux de télécommunications et fournisseurs de services de télécommunications de prêter leur concours technique au juge d'instruction.

Ensuite, comme pour l'article 88quater, l'article 90quater impose une sanction pénale à l'égard de la personne qui refuse de fournir la collaboration demandée, et soumet la personne requise au secret de l'instruction, dont la violation est réprimée conformément à l'article 458 du Code pénal. Par contre, contrairement à l'article 88quater, aucune dérogation n'est prévue au profit de l'inculpé ou de ses proches.

D. L'INTERCEPTION DES TÉLÉCOMMUNICATIONS

1) Bases légales

La loi nouvelle ne bouleverse pas le régime de l'interception des télécommunications, de leur repérage et de l'identification des appels. Elle en complète simplement, à trois égards, les dispositions applicables, conformément aux nouvelles dispositions introduites par la loi.

En ce qui concerne les écoutes de télécommunications tout d'abord, nous avons déjà abordé l'obligation de collaboration que le juge d'instruction peut imposer à certaines personnes disposant d'une compétence technique (article 90quater nouveau du Code d'instruction criminelle)[571]. La loi nouvelle complète le catalogue des infractions visées par la mesure (article 90ter, § 2), en y insérant les infractions visées par les articles 210bis, 259bis, 314bis, 324bis, 324ter, 504quater, 550bis et 550ter du Code pénal.

L'article 90septies nouveau concerne, quant à lui, les modalités de conservation des données résultant d'une écoute de télécommunications. Il précise ainsi que *« les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée et, dans la mesure du possible, pour réaliser sa transcription ou sa traduction. La même règle vaut pour la conservation au greffe des enregistrements et de leur transcription et pour les mentions dans le registre spécial. Le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, ces moyens et le moment où ils remplacent la conservation sous pli scellé ou le registre spécial prévus aux alinéas 3 et 4 »*.

Ensuite, l'article 109ter de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, se voit enrichit de précisions utiles au repérage des télécommunications et à l'identification des appels. L'alinéa 1 du paragraphe 2 est ainsi complété en vue de prévoir que le Roi fixe, par arrêté délibéré en Conseil des ministres, *« les obligations pour les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, dans les cas à déterminer par arrêté royal délibéré en Conseil des ministres et sur proposition du ministre de la justice et du ministre qui a les Télécommunications et les Entreprises et Participations publiques dans ses attributions, les données d'appel des moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications. Ce délai, qui ne peut jamais être inférieur à 12 mois, ainsi que les données d'appel et d'identification, seront déterminés par arrêté royal délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée.*

---

[571] Cf. supra.

Cette conservation imposée aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications doit s'effectuer à l'intérieur des limites du territoire de l'Union européenne ».

Les obligations précitées sont sanctionnées, en vertu de l'article 109ter E, § 3, nouveau, d'une peine d'emprisonnement de trois mois à six mois et/ou d'une amende de vingt-six francs à vingt mille francs.

Enfin, en vertu du paragraphe 4 nouveau de cette même disposition, *« le Roi par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée prévoit les modalités et moyens appropriés pour garantir la confidentialité et l'intégrité des données d'appel et d'identification visées au paragraphe 2 ».*

2) Analyse des nouvelles dispositions

Dans la mesure où la loi nouvelle ne fait qu'adapter l'arsenal législatif existant, relatif à l'interception des télécommunications, au repérage et à l'identification d'appels, sans cependant en bouleverser les principes, nous limiterons notre propos aux seules dispositions de la loi relative à la criminalité informatique.

a) L'article 11 de la loi nouvelle, complétant l'article 90ter, §2 du Code d'instruction criminelle

1°) Ratio legis

Afin de maintenir un équilibre entre la protection des droits fondamentaux de l'individu (comme le droit au respect de la vie privée) d'une part, et les nécessités de la lutte contre la délinquance d'autre part, le législateur subordonne le recours à l'interception des communications et des télécommunications à des conditions strictes. Parmi celles-ci figure l'exigence de proportionnalité, qui implique que cette mesure n'est admise que pour les infractions énumérées dans la liste exhaustive de l'article 90ter[572].

[572] H.D., BOSLY, D., VANDERMEERSCH, *Droit de la procédure pénale*, Brugge, La Charte, 1999, p. 301 et 320.

La fréquence des délits informatiques commis sur réseaux imposait, dans un souci d'efficacité de la répression[573], d'étendre l'article 90ter aux nouvelles incriminations (ou à un repérage par le Procureur du Roi en cas de flagrant délit).

Cette adjonction des délits informatiques au catalogue des infractions pouvant donner lieu à « écoute » s'inscrit, elle aussi, dans la ligne tracée par les Recommandations du Conseil de l'Europe[574].

2°) Commentaires

Les pouvoirs du juge d'instruction en matière d'interception des télécommunications sont désormais étendus puisque, en plus d'être permise vis-à-vis de faits constituant une infraction aux articles 259bis et 314bis du Code pénal, réprimant l'écoute, la prise de connaissance et l'enregistrement de communications et télécommunications privées, cette mesure sera applicable aux incriminations introduites par la loi nouvelle, à savoir le faux en informatique (article 210bis nouveau), la fraude informatique (article 504quater nouveau), l'accès non autorisé à un système informatique (article 550bis nouveau), et le sabotage informatique (article 550ter nouveau).

Les pouvoirs du juge d'instruction, en matière de repérage des télécommunications, ne font l'objet d'aucune restriction quant aux faits susceptibles de se voir appliquer la mesure. Ce n'est pas le cas du procureur du Roi qui, en vertu de l'article 88bis du Code d'instruction criminelle, ne peut en cas de flagrant délit que procéder à un repérage de télécommunications, limité aux infractions énumérées à l'article 90ter.

Dans ce contexte, l'élargissement de cette dernière disposition aux nouvelles infractions informatiques profite également au procureur du Roi.

b) L'article 12 de la loi, ajoutant un paragraphe 4 à l'article 90quater du Code d'instruction criminelle

Cette disposition impose une obligation de collaboration dans le chef de personnes dont le juge d'instruction *« présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance, ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique »*.

---

[573] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 29.

[574] Voy. le principe n°8 de la Recommandation R(95) 13 : *« Les droits de la procédure pénale doivent être révisés en vue de rendre possible l'interception des télécommunications et la collecte des données de trafic dans le cadre d'enquêtes sur des infractions graves contre la confidentialité, l'intégrité et la disponibilité des systèmes de télécommunications ou informatiques »*.

La Commission de protection de la vie privée estime qu'il faut veiller à ce que le respect du principe de proportionnalité soit respecté et que le décodage ou le décryptage ne soit fait que par la personne qui a connaissance du procédé de codage ou de cryptage, sans qu'il y ait de transmission d'informations relatives à ceux-ci[575].

Pour ce qui est de la disposition elle-même, celle-ci ayant précédemment fait l'objet de commentaires, nous nous permettons d'y renvoyer simplement[576].

c) L'article 13 de la loi, ajoutant un nouvel alinéa entre l'alinéa 4 et l'alinéa S de l'article 90septies du Code d'instruction criminelle

L'enregistrement et la conservation des données interceptées, quel que soit le type de télécommunications (informatique ou téléphonique) est réglé par l'article 90septies du Code d'instruction criminelle[577].

L'évolution des technologies aidant, de nouveaux procédés de conservation, de transcription ou éventuellement de traduction des enregistrements vont faire leur apparition (si ce n'est déjà fait). Les techniques de cryptage disponibles à l'heure actuelle peuvent d'ailleurs déjà être employées par les autorités judiciaires pour garantir la confidentialité et l'intégrité du matériel d'écoute[578] .

La loi nouvelle permet aux autorités judiciaires d'avoir recours, sous le vocable de *« moyens appropriés »*, à ces nouvelles technologies. L'exposé des motifs précise à cet égard que *« compte tenu des adaptations techniques et infrastructurelles nécessaires pour faire fonctionner les systèmes de sauvegarde de données sous plis scellés au greffe et remplacer le registre particulier et physique par son équivalent numérique, qui offrira plus de sécurité, le Roi est chargé de déterminer les modalités spécifiques et la date d'application »* de cet article[579].

Cette disposition n'étant pas spécifique à la criminalité informatique, nous ne la développerons pas dans cette analyse.

---

[575] Voy. J.-C., PAYE, « La loi relative à la criminalité informatique », Journ. proc., 21 septembre 2001, n°420, p. 15.
[576] Cf. supra.
[577] La conservation au greffe des enregistrements et de leur transcription et/ou traduction sous pli scellé sera complétée par la tenue d'un registre spécial par le greffier.
[578] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 29.
[579] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 30.

4) L'article 14 de la loi nouvelle, complétant l'article 109ter E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques

1°) Ratio legis

Le principal obstacle à la poursuite de la criminalité informatique commise au moyen des télécommunications réside dans la difficulté d'identifier l'auteur du délit, celui-ci bénéficiant du relatif anonymat que permet l'usage des réseaux informatiques.

L'identification du délinquant suppose que les autorités judiciaires disposent de l'adresse IP[580] utilisée par celui-ci lors de son passage sur le réseau, de même que de l'heure et de la date de sa connexion. Dans cette optique, le magistrat peut imposer aux fournisseurs de services ou aux opérateurs de réseaux de télécommunications de leur délivrer ces informations.

Le problème qui se pose alors est que, en l'absence de disposition légale les astreignant à une quelconque obligation en la matière, les opérateurs et fournisseurs de services sont libres de déterminer la durée de conservation des données d'appel et d'identification. Les autorités judiciaires risquent donc de ne pas recevoir les informations demandées si la demande est formulée plusieurs mois après la communication concernée.

Pour remédier à ce problème récurrent, la loi nouvelle impose aux fournisseurs de services et opérateurs de réseaux de télécommunications, sous la menace d'une sanction pénale, l'obligation de conserver, durant une période d'au moins douze mois, les données d'appel et les données d'identification des moyens de télécommunications[581].

2°) Commentaires

- Quant aux destinataires de l'obligation d'enregistrement et de conservation

La disposition nouvelle vise tant les opérateurs de réseaux de communications que les fournisseurs de services de télécommunications. Ces notions étant définies aux articles 68, 5°bis, 68, 23°, et 68, 19° de la loi du 21 mars 1991, il en résulte que les services concernés concernent tous les services de communications, qu'il s'agisse de téléphonie classique ou mobile ou d'informatique.

De plus, les travaux préparatoires renvoient également à la Recommandation R (95) pour la détermination du contenu de ces notions. Le prestataire (le fournisseur) de services y est décrit comme *« 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*

[580] Cf. lexique en annexe.

» et l'opérateur comme celui *« qui est responsable du transport des données sur une infrastructure de télécommunications »*[582].

Ainsi, si Belgacom peut être considéré comme opérateur de télécommunications, la catégorie des fournisseurs de services englobe tous les fournisseurs de courrier électronique, les services d'accès, les services de forums de discussions ou les prestataires offrant des services à valeur ajoutée (services de cryptographie, de trusted third parties, services électroniques bancaires,...)[583].

Par contre, selon Meunier, les cybercafés ne devraient pas se voir figurer dans cette catégorie, puisqu'ils n'acheminent ni ne transmettent, à proprement parler, de données informatiques, mettant simplement du matériel informatique[584].

Si nous adhérons à cet avis, nous soulignons néanmoins que certaines mesures devraient être imposés vis-à-vis des cybercafés afin qu'ils stockent certaines informations concernant leurs clients. Par « informations », nous visons, par exemple, une photocopie de la carte d'identité, avec la date et l'heure de connexion, au risque pour ceux-ci de se voir poursuivis en lieu et place des criminels informatiques, l'adresse IP retrouvée renvoyant au cybercafé[585].

- Quant à l'objet de l'obligation imposée aux opérateurs et fournisseurs

Les opérateurs et fournisseurs sont tenus d'enregistrer et de conserver les *« données d'appel de moyens de télécommunications »* et les *« données d'identification d'utilisateurs de services de télécommunications »*.

Nous ne pouvons que regretter le caractère pour le moins vague de ces notions de données « d'appel » et « d'identification », et l'absence de précisions légales à ce sujet. Bien que l'article 109ter renvoie au Roi pour préciser ces concepts, le Conseil d'État avait estimé qu'un arrêté royal n'était pas une base légale suffisante, dans la mesure où sont concernés des éléments participant à la vie privée de chacun[586].

Ces critiques ont été relayées par la Commission pour la protection de la vie privée, se fondant sur la nécessité d'une loi requise par l'article 22 de la Constitution[587]. Le gouvernement a

---

[581] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 30.
[582] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 61.
[583] Conseil de l'Europe, *Problèmes de procédure pénale liés à la technologie de l'information. Recommandation n°R (95) 13 et exposé des motifs*, éd. du Conseil de l'Europe, 1996, p. 61.
[584] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, p. 657.
[585] Certains cybercafés recourent à cette pratique, mais pas l'ensemble d'entre eux.
[586] Avis du Conseil d'Etat, *Doc. parl*., Ch. repr., 0213/001, p. 56.
[587] Voy. J-C., PAYE, « La loi relative à la criminalité informatique », Journ. proc., 21 septembre 2001, n°420, pp. 13 à 14.

finalement opté pour une position intermédiaire, selon laquelle il revient au Roi de préciser le contenu des données visées, après avoir pris l'avis de cette dernière Commission.

En ce qui concerne les données d'appel, l'exposé des motifs précise qu'il s'agira des données relatives à l'origine, la destination, la durée, la localisation des appels[588] .

Dès lors, si des informations telles que les adresses IP rentrent dans cette acception, nous ne pensons pas que c'est le cas de l'historique des sites Internet visités. A moins d'être indispensables pour les besoins de l'enquête, la consultation de ceux-ci nous paraît constituer une violation du droit au respect de la vie privée tel que défendu par l'article 22 de la Constitution.

La loi nouvelle ajoute que ces données doivent être conservées *« en vue de l'investigation et de la poursuite d'infractions pénales »*. Cette précision n'a d'autre fonction que d'insister sur la finalité pénale de la mesure, les données ne pouvant donc être collectées à des fins purement statistiques par exemple.

- Quant à la durée de conservation des données d'appel et des données d'identification

L'article 109ter E, § 2, alinéa 1, de la loi du 21 mars 1991 prévoit que l'obligation de conservation des données s'impose pendant un délai qui sera déterminé par le Roi par arrêté royal délibéré en Conseil des ministres après avis de la Commission pour la protection de la vie privée, mais ne pouvant être inférieur à 12 mois.

La fixation de ce délai a fait l'objet de vives discussions au Parlement entre les défenseurs de deux thèses radicalement opposées.

Les tenants de la première thèse estimaient que l'obligation de conserver les données d'appel et les données d'identification était, d'une part, attentatoire à la vie privée des personnes concernées par ces données, et, d'autre part, risquait d'impliquer des coûts importants pour les fournisseurs de services et les opérateurs[589]. De plus, selon la Commission de protection de la vie privée, le risque est grand de voir se constituer, en raison de la durée de conservation des données, de véritables banques de données à caractère personnel[590].

---

[588] Projet de la loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl*., Ch. repr., sess. ord. 1999-2000, 0213/001 , p. 30.

[589] Voy. l'avis de la Commission européenne qui estime que *« lesdites obligations sont en effet susceptibles de gêner, de rendre plus onéreux et donc de rendre moins attrayant l'exercice d'activités économiques consistant en la prestation de services de la société de l'information par un opérateur d'un Etat-membre qui voudrait s'établir ou offrir ses services en Belgique »* (avis de la Commission européenne, *Doc. parl*., Ch. repr., 0213/011, p. 18).

[590] Voy. J-C., PAYE, « La loi relative à la criminalité informatique », Journ. proc., 21 septembre 2001, n°420, p. 15.

Les partisans de cette thèse concluaient à la nécessité de prévoir un délai de conservation relativement bref, par exemple de trois mois, à l'image de ce que prévoient certaines législations étrangères, comme l'Allemagne, et de ce que préconise la Recommandation 3/99 *« relative à la conservation des données relatives aux communications pour les offreurs de service Internet en vue d'assurer le respect de la loi »*[591].

Les partisans de la seconde thèse étaient par contre d'avis que, dans le souci de garantir l'efficacité des enquêtes pénales en milieu informatisé, il convenait de prévoir un délai plus long, d'au moins douze mois. Cette tendance l'a finalement emporté, étant entendu que ce délai de douze mois constitue un minimum, qui pourra encore être allongé par arrêté royal[592].

Cette solution, plus réaliste, nous paraît devoir être approuvée du point de vue pénal, et ce pour plusieurs raisons.

Tout d'abord, en fonction des éléments dont il dispose au début de l'enquête, le magistrat peut ne pas percevoir immédiatement la nécessité de procéder à un repérage de télécommunications et/ou à une identification. De même, les autorités judiciaires peuvent n'être saisies d'une plainte de la victime que de nombreux mois après les faits. Une obligation de conservation trop réduite risquerait, dans ces hypothèses, d'anéantir toute chance d'identification de la personne visée.

Ensuite, l'étendue géographique des réseaux internationaux, en particulier du réseau Internet, a pou conséquence que la criminalité informatique présente très fréquemment un caractère transfrontalier. Dès lors, en l'absence de convention internationale autorisant le recours à un mécanisme plus souple de coopération, l'administration de la preuve suppose le recours à la commission rogatoire. Cette mesure, particulièrement lourde, risque elle aussi de faire échec à l'instruction si l'obligation de conservation imposée aux opérateurs est conçue trop restrictivement[593].

Enfin, sur un plan pratique, bien que Peter Van Roste, porte-parole de l'ISPA, l'association des fournisseurs d'accès en Belgique déclare que *« jamais* (il n'a) *rencontré un cas où l'enquête devait remonter plus de trois à six mois en arrière »*[594], ce problème s'est régulièrement posé lors du stage que nous avons effectué à la Computer Crime Unit de Bruxelles en 2000. En effet, Peter Van

---

[591] Cette recommandation a été élaborée par le « Groupe pour la protection des personnes pohysiques à l'égard du traitement des données à caractère personnel », institué par la directive 95/46/CE du Parlement européen et du Conseil de l'Europe, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

[592] Voy. C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, pp. 658 à 659.

[593] Voy. les préoccupations exprimées à ce sujet par un membre de l'ancienne National Computer Crime Unit (devenue depuis la Federal Computer Crime Unit), lors de son audition par le Sénat (*Doc. parl*., Ch. repr., 0213/011, p. 11).

Roste ne paraît pas être au courant que l'arriéré judiciaire en Belgique est tel qu'il arrive fréquemment que les enquêteurs doivent attendre plusieurs mois avant d'obtenir un réquisitoire du juge d'instruction, si bien que le délai de trois mois est souvent beaucoup trop court.

Ce débat illustre la difficulté qu'il peut y avoir à concilier des intérêts fondamentalement divergents comme la vie privée des utilisateurs de services et réseaux de télécommunications, d'une part, et la protection de l'ordre public, d'autre part.

- Quant aux sanctions pénales

La sanction prévue à l'article 109ter E, § 3, frappe les fournisseurs et les opérateurs qui ne conserveraient pas tout ou partie des données d'appel et d'identification, qui les garderaient pendant un délai inférieur à 12 mois, ou les stockeraient en dehors du territoire de l'Union européenne.

Cette incrimination étant une infraction réglementaire, elle est punissable même si l'auteur n'était pas animé d'un dol. Elle pourrait donc s'appliquer au fournisseur de services ou à l'opérateur qui néglige d'enregistrer les données et de les stocker, qui les conserve durant une période insuffisante ou qui n'enregistre qu'une partie des informations pertinentes[595].

[594] JENNOTTE, A., « La Net-police tracera chaque internaute », Le Soir, 11 août 2000.
[595] C., MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique », Act. dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, pp. 157 et 158.

Titre III – L'action policière : Analyse empirique de la Computer Crime Unit

Cette partie sera consacrée à l'action de la police belge en charge de la criminalité informatique, à savoir la Federal Computer Crime Unit (FCCU) et les Computer Crime Units (CCU's).

Cette partie sera principalement composée d'éléments empiriques, récoltés lors de notre stage au sein de Computer Crime Unit de Bruxelles en 2001, mais également d'éléments issus de documents internes aux services de police et d'interviews de fonctionnaires de police travaillant au sein de ces unités parues dans la presse. Nous préciserons, à chaque fois, l'origine de nos sources.
Certains éléments peuvent avoir changé depuis notre stage, bien que, d'après nos contacts récents avec les membres de la CCU de Bruxelles, les choses soient généralement restées en l'état.

Cette analyse, qui ne se voudra pas exhaustive, étant entendu la durée de notre stage (trois mois), aura principalement pour but de montrer que la loi nouvelle risque de voir son application handicapée par le manque de moyens dont disposent les services de polices. Ce manque de moyens sera pointé tant sur le plan humain que matériel.

Nous insisterons également sur le fait que cette pénurie de moyens, outre une application plus difficile de la loi, va entraîner les autorités judiciaires dans un cercle vicieux, les cantonnant à s'occuper d'affaire ne nécessitant pas, quant à leur résolution, d'investissement très importants, mais qui, à terme, aboutiront à une somme de travail supplémentaire considérable.

Enfin, nous terminerons par quelques considérations succinctes relatives à l'apport de la loi nouvelle à la procédure pénale. Cette partie sera plus théorique, étant entendu qu'à l'époque de notre stage, celle-ci venait à peine d'entrer en vigueur, et que nous n'avons dès lors pas eu l'occasion d'assister à son application.

Section 1 – Historique de l'institution

Une des premières situations où l'ancienne gendarmerie fit appel aux informaticiens paraît aujourd'hui des plus anachroniques. L'ordinateur personnel analysé coûtait à cette époque 300.000 francs belges (soit environ 7500€) et ne disposait même pas d'un disque dur.
Jusqu'au début des années 1990, les demandes d'assistance relatives à l'informatique étaient plutôt rares, et il suffisait alors de faire appel aux gendarmes informaticiens du Centre de traitement de l'Information de la Gendarmerie, ou à la direction supérieure de la télématique[596].

Les années 1990 furent marquées par une certaine explosion de la criminalité informatique, amenant à la création d'unités spécialisées.
En 1992, la police judiciaire créait ainsi les Computer Crime Units (CCU's), chapeautées à partir de 1997 par la National Computer Crime Unit (NCCU).
La gendarmerie, quant à elle, organisait, à partir de 1995, le team Assistance pour la Recherche en Environnement Automatisé (AREA), opérationnelle au sein du Bureau Central de Recherches (BCR).

En 2001, année de la réforme des polices, les équipes AREA et NCCU fusionnent pour constituer le Federal Computer Crime Unit (FCCU), qui chapeaute désormais les CCU's régionales. Elles sont actuellement au nombre de 17, réparties à travers le territoire, chaque arrondissement judicaire ne disposant donc pas d'une CCU.

Section 2 – Organisation de l'institution

« L'organisation et l'action des Computer Crime Units, tant au niveau fédéral que régional se doivent de garantir :

- une assistance efficace aux services de police dans le cadre de dossiers judiciaires, afin de rechercher toute information pertinente dans un environnement ITC[597], de sauvegarder celle-ci et la mettre à disposition des enquêteurs sous une forme lisible et compréhensible.

- La lutte efficiente contre toutes les formes de criminalité dans un environnement ICT, et ce, tant par le biais de la spécialisation et de la prévention que par des interventions proactives et réactives, dans le but de réduire le plus possible l'impact négatif de ces formes de criminalité sur la société »[598].

---

[596] L., BEREINS, « A la recherche des bits criminels, Enquêtes digitales », Politea, Bruxelles, octobre 1998, n°8, p. 9.
[597] ICT désigne la « technologie de l'information et de la communication ».
[598] L., BEREINS, *Fiche d'information concernant l'organisation et le fonctionnement du Féderal Computer Crime Unit et des Computer Crime Units régionaux*, Bruxelles, Direction de la lutte contre la criminalité économique et financière, 10 juillet 2001, p. 2.

Au niveau national, la FCCU se situe au sein de la Direction de la Lutte contre la Criminalité Economique et Financière (DJF).

Au plan régional, les CCU's font partie de la capacité de la Recherche fédérale qui dépend des Directeurs judiciaires d'arrondissement[599].

Les CCU's sont compétentes, notamment, pour les domaines suivants :

- les infractions à la loi « Belgacom » du 21 mars 1991 ;
- les infractions à la loi du 30 juin 1994 portant sur la protection des programmes d'ordinateurs ;
- les infractions à la loi du 28 novembre 2000 relative à la criminalité informatique[600].

[599] L., BEREINS, *Fiche d'information concernant l'organisation et le fonctionnement du Féderal Computer Crime Unit et des Computer Crime Units régionaux*, Bruxelles, Direction de la lutte contre la criminalité économique et financière, 10 juillet 2001, p. 2.

[600] L., BEREINS, *Fiche d'information concernant l'organisation et le fonctionnement du Féderal Computer Crime Unit et des Computer Crime Units régionaux*, Bruxelles, Direction de la lutte contre la criminalité économique et financière, 10 juillet 2001, p. 3.

Section 3 – Analyse empirique proprement dite

A. LES MISSIONS DE LA CCU

Concrètement, la CCU de Bruxelles est divisée en sous-sections informelles, fonctions de la parité linguistique et de la spécificité des affaires, ceci n'empêchant absolument pas les échanges entre elles.

Saisie principalement par plainte[601], la CCU est principalement confrontée à des affaires de pédophilie et de faux en informatiques (fausses cartes de crédit, CD pirates,...), ainsi qu'à de toute une série de problèmes « mineurs », comme l'envoi de SMS d'insultes.

Les inspecteurs de la CCU ont également une mission d'assistance des autres sections de la police judiciaire, à la demande de celles-ci, lorsque les affaires traitées comportent des aspects « technologiques », à quelque niveau que ce soit (saisie de PC, analyse de répertoire GSM, analyse d'agenda électronique,..).

Sur ce point, il nous faut souligner qu'étonnement, la plupart d'entre eux n'ont pas suivi pas de formation d'informaticiens. Hormis quelques exceptions, la plupart de ces inspecteurs viennent d'univers (assistant social, ingénieur,...) ou de sections différentes (criminelle, financière,...), et sont majoritairement autodidactes.

Ce n'est pas le cas de l'ensemble des membres des CCU's, certains étant les concepteurs des programmes utilisés aussi bien lors des perquisitions, que ceux utilisés dans la brigade (registre des PV, ...), mais ils sont une minorité.

Comme nous venons de le dire, la CCU est principalement saisie sur plainte. Ce n'est pas une obligation, mais les inspecteurs nous ont expliqué avoir bien assez de travail sans qu'il soit nécessaire d'utiliser les possibilités offertes par la proactivité.

En effet, sur le plan pratique, leurs missions consistent à effectuer les perquisitions, à analyser les ordinateurs saisis, à interroger les suspects, les victimes, à venir en appui d'autres sections de la police, mais également à répondre aux questions des citoyens, des journalistes, de leurs collègues[3],..., si bien que les inspecteurs déplorent l'absence de personnel administratif

Ces tâches ne nécessitent d'ailleurs pas toutes de grandes compétences (ex : consulter des photos pédophiles, vérifier la présence de MP3 sur un disque dur,...), si bien que certaines d'entre elles pourraient être déléguées à un personnel moins « spécialisé ». Nous y reviendrons.

---

[601] Nous y reviendrons plus loin.

B. LES PROBLÈMES RENCONTRÉS PAR LA CCU

Nous avons classé les divers problèmes rencontrés par la CCU par « secteurs » touchés, une classification par ordre d'importance étant particulièrement difficile de par le fait que le caractère plus ou moins nuisible d'un problème dépend avant tout de la situation et du moment.

a) Le manque de moyens matériels

La caricature montrant des délinquants mieux équipés que les policiers chargés de les arrêter ne devraient plus nous faire sourire, celle-ci se rapprochant dangereusement de la réalité.

Lors de notre stage (en 2001), nous avons ainsi constaté que :

- Les inspecteurs travaillent à 2 sur une imprimante (dont la vitesse d'impression est d'une page à la minute !)
- Ils doivent « justifier » l'encre utilisée, si bien que les rapports sont souvent exempts de photos (ou alors celles-ci se voient réduites au minimum minimorum). Or, dans certains dossiers, les photos sont indispensables (pédophilies, sites piratés, contrefaçon, ...).
- Ils ne possèdent que 2 portables pour l'ensemble de la CCU, cette pénurie posant quelques problèmes lorsqu'il s'agit de prendre la déposition de plusieurs personnes sur les lieux du crime ou lors des perquisitions.
- De même, on ne trouve qu'un graveur de CD externe à la CCU. Difficile dès lors de profiter des possibilités de la nouvelle loi sur la criminalité informatique (copie de l'ensemble du disque dur, des informations situées sur le réseau,...).

Olivier Bogaert, inspecteur principal à la FCCU déclarait d'ailleurs à ce sujet que *« récemment, nous avons saisi un disque dur de 60 gigas qu'il aurait fallu sauvegarder sur un support de taille identique ou supérieure. Malheureusement, nos disques durs ne dépassent pas les 40 gigas. Nous avons donc du bricoler une solution pour pouvoir stocker l'information sur plusieurs supports »*[602].

Ce type de problèmes matériels, quotidiens, engendre des pertes de temps finissant par cantonner les enquêteurs dans un travail réactif.

A ces considérations matérielles, il nous faut ajouter un problème d'ordre organisationnel, à savoir que la CCU joue également le rôle de Help-Desk pour l'ensemble de la brigade !

Pour citer Olivier Bogaert, *« c'est comme si la section financière s'occupait de la comptabilité de la PJ »*[603].

---

[602] V., GENOT, « La cyberpatrouille », Le Vif/L'Express, 1er mars 2002, p.24.
[603] Entretien avec l'inspecteur principal Bogaert, 15 mars 2001.

Concrètement cela signifie que plusieurs fois par jour les inspecteurs de la CCU reçoivent de coups de téléphone de collègues leur demandant de venir réparer un PC, d'installer une imprimante, de configurer un modem, ...

De même, lorsqu'ils n'ont pas le temps de se déplacer, ce sont leurs collègues qui le font. Nous avons ainsi vu défiler cinq inspecteurs de la PJ venir scanner des photos de personnes disparues, monopolisant le scanner de la CCU et un inspecteur de la CCU (pour le faire fonctionner), car celui de la PJ n'était pas installé !

b) Le manque de formation et de moyens humains

• Comme nous l'avons déjà souligné, les tâches de la CCU ne nécessitent pas toutes d'être un informaticien confirmé. Certaines sont en effet des plus simples, accessibles à n'importe quel inspecteur ayant suivi une formation élémentaire. Il s'agira, par exemple, de vérifier la présence sur un ordinateur de fichiers à caractère pédophiles, de les répertorier et d'imprimer certains de ceux-ci, de constater la présence de matériel de contrefaçon,…

Mais cette formation n'existe pas, que ce soit au niveau local ou fédéral. Les futurs inspecteurs de la CCU sont choisis en fonction de leurs connaissances informatiques préalables à leur passage à l'école de police : cela ne fait pas partie de leurs cours. Si bien que feront partie de la CCU ou de la FCCU que les « informaticiens » ayant envie de travailler à la police.

On trouve bien des néophytes désireux d'approfondir leurs connaissances, mais ils seront plus un poids supplémentaire en terme de temps perdu qu'une véritable aide venant soulager les membres de la CCU de leur charge de travail.

Quant au personnel civil, s'il est souvent réclamé par les enquêteurs, les fonctionnaires interrogés à ce sujet nous ont répondu qu'il manquait un budget pour ce type de personnel, et que de toutes manières, la direction de la police judiciaire ne semblait pas très intéressée par cette idée[604].

Cette manière de faire nous semble étonnante, étant donné que d'autres sections emploient du personnel civil[605].

• Si les inspecteurs de la CCU sont pour la majorité des passionnés d'informatiques, ce n'est pas toujours (pour ne pas dire jamais) le cas au niveau local.

---

[604] Entretien avec les enquêteurs, 15 mars 2001.

[605] La direction de la police judiciaire ne nous étant pas facilement accessible, nous n'avons pas pu éclaircir ce point.

Olivier Bogaert nous expliquait ainsi que lorsque le local trouve, à l'occasion d'une affaire, un ordinateur, un GSM, un agenda électronique,..., il contacte immédiatement la CCU afin qu'elle fasse les vérifications nécessaires. Olivier Bogaert déplorait ainsi le manque de formation des inspecteurs au niveau local, la majorité des ces vérifications étant des plus simples (vérification de mail, consultations de sites Internet, de répertoires GSM,...).

- L'intervention d'un magistrat est nécessaire dans toute enquête. Pour solliciter celle-ci, les inspecteurs exposent les faits et le type d'aide qui leur est nécessaire. Or, il arrive souvent que les inspecteurs de la CCU soient amenés à introduire des informations, des explications techniques dans leurs procès-verbaux, et ce même pour les infractions les plus simples (par exemple, l'envoi d'insultes par SMS via un site Internet). Le problème est que les magistrats n'ont pas tous les connaissances suffisantes que pour comprendre l'objet du problème, si bien qu'un PV de deux pages se transforme bien souvent en un exposé de dix pages. Pour l'exemple, nous citerons la tentative d'explication concise d'une fenêtre Popup, qui nécessita schémas, copies d'écrans d'ordinateur et explications détaillées.

Ce manque de formation est également générateur de pertes de temps considérables et quotidiennes.

c) L'impunité des « gros » hackers et la création d'un cercle vicieux

Le résultat des ces différents problèmes est simple à déterminer. Les enquêteurs, occupés à charges « mineures », satellites de leur mission première d'enquête et de recherche du crime, disposeront de moins de temps pour les affaires complexes.

Ainsi, si les inspecteurs de la CCU passent de temps à autre à la télévision à l'occasion de l'arrestation d'un Red Attack ou assimilé, la majeure partie de leur travail consiste à localiser l'origine d'insultes par SMS, à faire procéder à l'annulation de faux-profils sur des sites de rencontres, à répondre aux journalistes concernant le « fléau MP3 »,…

En conséquence, la CCU déplore l'absence d'une sorte de filtrage des affaires par le local, leur permettant de se concentrer sur les affaires nécessitant de gros moyens, de grandes connaissances,...

Selon les inspecteurs principaux Bogaert et Link, sans cela, il ne sera pas possible de répondre à la demande de sécurité « informatique » des années à venir[606]. Car, rappellons-le, si le nombre de pirates et les moyens dont ils disposent croissent de manière exponentielle, ce n'est pas du tout le cas de la CCU.

[606] Entretien avec les enquêteurs, 7 mars 2001.

Ce problème entraîne ipso facto une sorte d'impunité de fait pour les gros hackers. Ceux-ci utilisant des techniques plus subtiles, sont moins visibles, plus prudents, en somme plus « professionnels », les affaires les concernant demandent beaucoup de moyens en temps et en personne. Et comme les inspecteurs ne disposent ni de l'un, ni de l'autre, la CCU se retrouve ainsi prise dans un cercle vicieux : elle s'occupera principalement d'affaires mineures qui, si elles ne demandent pas toujours beaucoup de moyens pour être résolues[607], font néanmoins perdre un temps précieux aux enquêteurs (pour la rédaction des PV, la demande de réquisitoire, la réponse des administrateurs, l'audition des victimes, des auteurs,…), si bien que ceux-ci ne pourront s'attaquer aux affaires complexes que subsidiairement, celles-ci nécessitant des moyens plus importants[608], lorsqu'il en auront les moyens, sur le plan matériel, humain et temporel, et, ceci entraînant, de facto, qu'ils se rabattent à nouveau sur les petites affaires, et ainsi de suite.

Certes de grosses affaires sont résolues (comme l'affaire RedAttack par exemple), mais leur faible nombre[609], comparé à celui des affaires mineures, démontre bien qu'il s'agit d'exception.

A titre d'exemple, l'enquête amenant à l'arrestation d'un pirate informatique spécialisé dans le deface de site a duré plus d'un an et demi, les enquêteurs étant continuellement interrompus dans leur travail par des charges annexes, comme celles qui viennent d'être décrites.

---

[607] Par exemple, pour trouver l'auteur d'un SMS anonyme, il suffira aux enquêteurs de disposer d'un réquisitoire du juge d'instruction commandant aux administrateurs du site de livrer les données relatives aux adresses IP des internautes (correspondant à l'heure d'envoi des SMS) aux enquêteurs. Pour rappel, les adresses IP contiennent diverses informations, comme le lieu de connexion, l'heure à laquelle elle a été établie, sa durée, le type de connexion,…

[608] Il leur faudra par exemple infiltrer les groupes de pirates, procéder à des écoutes téléphoniques,…

[609] Entretiens avec l'inspecteur principal Charles Link, 20 mars 2001.

C. L'APPORT DE LA LOI DU 28 NOVEMBRE RELATIVE À LA CRIMINALITÉ INFORMATIQUE

La loi sur la criminalité informatique, nonobstant les remarques qui viennent d'être faites concernant le manque de moyens, permet désormais aux inspecteurs d'enquêter plus facilement sur les actes de délinquance informatique.

Préalablement à cette loi, lorsqu'ils désiraient, par exemple, poursuivre une personne gravant des CD pirates, les enquêteurs devaient recourir aux articles du Code pénal consacré au faux « classique » (articles 193 et suiv. du Code pénal). Si cette pratique était courante, elle n'était pas pour autant pratique, comme nous l'avons vu dans l'analyse de la loi, dépassée par rapport aux possibilités offertes par les nouvelles technologies.

Olivier Bogaert nous expliquait d'ailleurs à ce sujet que la nouvelle loi étant grandement attendue par les enquêteurs, ceux-ci devant jusqu'alors travailler par analogie avec des lois existantes, si bien que le hacker était encore, il y a peu, poursuivi pour vol de données[610].

La nouvelle loi a ainsi pallié à ce problème en définissant précisément les infractions poursuivies.

De même, en ce qui concerne la saisie et les perquisitions, de réelles innovations étaient nécessaires, en raison du caractère extrêmement mouvant des données informatiques.

C'est ainsi que l'apport le plus utile de la nouvelle loi est certainement les possibilités offertes concernant la saisie informatique. Désormais, il est possible de saisir des données présentes sur un autre ordinateur que celui faisant l'objet de la saisie, pour autant que ceux-ci soient connectés[611].

D'autres obligations de collaboration, notamment pour les responsables de systèmes informatiques faisant l'objet d'une enquête existent. Un arrêté royal détermine ainsi dans quels cas et pendant combien de temps les fournisseurs d'accès, de services, devront enregistrer et conserver les données relatives à la connexion et à l'identité des internautes. Ces obligations ne seront pas plus développées ici, n'ayant pas fait l'objet d'application durant notre stage.

---

[610] Entretien avec les enquêteurs, 27 février 2001.

[611] Nous renvoyons à l'analyse de la loi pour de plus amples développements.

Conclusion

Il est clair que le manque de moyens matériel et humains constitue le principal problème de la CCU. Comme nous l'avons expliqué, avec plus de moyens et plus d'hommes, les affaires seraient mieux traitées, plus rapidement,...

Ce manque de moyens est à déplorer tant au sein de la CCU que dans les services avec lesquels elle collabore. Ainsi, par exemple, s'il y avait plus de juges d'instruction, les réquisitoires seraient plus rapidement rédigés, les informations seraient plus rapidement récoltées et les affaires plus rapidement réglées. Un exemple parmi d'autres.

De même, comment imaginer lutter à armes égales contre les pirates informatiques, par nature à la pointe du progrès, lorsque l'on dispose d'un matériel vieux de presque 10 ans ?

Ces éléments nous amène à poser la question de la politique criminelle observée par la CCU.

Elle est assez simple : elle n'a pas de cibles privilégiées, pas de secteurs réservés. Du moins officiellement.

Officieusement, les choses sont très légèrement différentes, conséquences de toute ce qui a déjà été dit précédemment. L'essentiel de la « clientèle » de la CCU sera composée de petits farceurs et autres enquiquineurs, et rarement de véritables criminels informatiques.

Dès lors, si la loi apporte les modifications souhaitées par les enquêteurs eux-mêmes, il faudrait également leur donner les moyens d'appliquer celle-ci, sans quoi la situation restera (pratiquement) inchangée dans les faits.

Deux solutions nous semblent devoir être envisagées pour régler, du moins partiellement, les problèmes rencontrés par la CCU.

D'une part, une véritable formation au sein de l'école de police en fonction de l'affectation que les futurs enquêteurs auront privilégiée nous semble un point fondamental. Aujourd'hui, l'informatique est devenu à ce point important qu'une police qui se veut efficace et en accord avec son époque ne peut se permettre de courir de services en services pour des problèmes mineurs.

D'autres part, dans le même ordre d'idées, quantité de tâches ne nécessitent pas un bagage juridique, judiciaire pour être accomplies. Que ce soit pour des travaux de secrétariat (téléphones, prises de rendez-vous, planning,...) ou des travaux de maintenance informatique (dépannages de PC, installation de nouveau matériel,...), un personnel civil nous semble également une solution raisonnable et avantageuse pour chacun.

Enfin, le caractère proactif de la loi restera lettre morte tant que tous ces problèmes n'auront pas été réglés, ce qui, à notre sens et en accord avec les enquêteurs, n'est pas près d'arriver. Car si les organes étatiques ont pris conscience de l'ampleur du phénomène et l'ont traduite sur le plan législatif, la réponse en terme de moyens se fait toujours attendre.

Conclusion sur la loi du 28 novembre 2000 relative à la criminalité informatique

Bien que la criminalité informatique soit, comme nous l'avons vu, caractérisée par le chiffre noir, nous ne pensons pas trop nous avancer en lui prédisant une croissance constante dans les années à venir, consécutive de l'évolution des nouvelles technologies[612].

L'adaptation du Code pénal et de la procédure pénale aux nouvelles technologies, réclamée tant par la jurisprudence et la doctrine que par les instances internationales, s'est traduite par l'élaboration et l'adoption de la loi du 28 novembre 2000 relative à la criminalité informatique.

Bien qu'elle soit tardive, en comparaison de certains de nos voisins comme la France ou les Pays-Bas, cette loi est néanmoins avant-gardiste, comme en témoigne notamment ses références au projet de Convention du Conseil de l'Europe sur la cybercriminalité, et témoigne du souci constant de ne pas se voir dépasser par des progrès techniques à venir qui la rendrait, à son tour, inadaptée.

Ce souci amène le législateur à certains biais qu'il nous faut à présent souligner.

Tout d'abord, avançant la volonté de rester aussi neutre que possible pour être applicable à toutes les situations futures, le législateur s'est gardé de définir un ensemble de notions, au premier rang desquelles figure la criminalité informatique elle-même ! Nous trouvons pour le moins paradoxal de légiférer dans une matière n'ayant pas été clairement définie. De même, les notions essentielles de « donnée informatique » et de « système informatique » ne sont pas définies, alors que le texte de loi y fait constamment référence, ouvrant ainsi la porte à de futures interprétations divergentes, qui seront autant de sources potentielle d'insécurité juridique.

Concernant la procédure pénale ensuite, les mêmes défauts sont à pointer. Ainsi, par exemple, le législateur n'a pas défini clairement le régime juridique la recherche informatique, alors qu'il précise les modalités d'extension de celle-ci.

Enfin, et nous y reviendrons dans la conclusion générale de cet exposé, le législateur, peut-être dépassé par les particularités du réseau, n'a pas hésité à s'octroyer certains droits, comme celui relatif à la perquisition dans un système de données situer à l'étranger, au mépris des conventions et accords internationaux et du respect de principes fort comme le respect de la vie privée.

Cette bi présente également, à notre sens, beaucoup de points intéressants et bien sentis. Tout d'abord, les dispositions nouvelles et l'adaptation du Code pénal sont particulièrement appréciés par

---

[612] Voy. P., ROSE, *La criminalité informatique à l'horizon 2005. Analyses prospectives*, Paris, L'Harmattan, 1992.

le monde judiciaire, permettant à celui-ci de se remettre dans la course face au progrès des criminels informatiques et de s'attaquer désormais à des infractions difficilement incriminables sous l'ancien Code pénal.

En outre, contrairement à une certaines partie de la doctrine, l'absence de dol spécial en ce qui concerne l'infraction d'accès non autorisé aux systèmes informatiques nous paraît être particulièrement pertinente, au regard de ce que nous savons désormais sur les motivations des hackers, notamment concernant la notion de jeu et de défi.

Si certains considèrent que cette disposition ouvre la voie à l'incrimination de la « simple curiosité »[613], nous ne voyons pas quant à nous où se situe le problème, étant donné qu'il est impossible de s'introduire « par hasard » dans un système informatique. De même, nous ne pensons pas que cette disposition aurait soulevé autant de contestations dans d'autres domaines que la criminalité informatique : peu de personnes auraient ainsi critiqué une disposition punissant les personnes qui s'introduisent dans votre domicile par curiosité.

Enfin, et c'est un lieu commun, il nous faut souligner que si cette loi se veut efficace, le législateur devra se donner les moyens de sa politique. Ainsi, le manque moyens mis à la disposition des CCU's, le manque de magistrats, le manque de formation du personnel, sont autant de facteurs amenant à une mauvaise application de la loi. Car si, encore une fois, certaines dispositions nous paraissent tout à fait pertinentes, comme l'obligation de conservation des données d'appel et d'identification pendant une période d'au moins 12 mois, il nous semblerait regrettable de voir celles-ci perdre de leur utilité confrontées à la réalité du terrain et des carences de l'appareil judiciaire.

Il nous reste à espérer qu'après avoir pris conscience de l'importance d'une législation spécifique à la criminalité informatique, le législateur prendra compte des carences existant en la matière et qu'il prendra les mesures nécessaires pour y remédier, afin de propulser la Belgique sur le devant de la scène en matière de lutte contre la criminalité informatique.

---

[613] Voy. F., DE VILLENFAGNE, S., DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs & Medias*, 2001, pp. 81.

Conclusion générale

Il est à présent temps pour nous de conclure cet exposé et d'apporter la réponse à notre question principale concernant la pertinence des moyens mis en œuvre pour lutter contre la criminalité informatique.

Nous avons commencé cet exposé en analysant les risques informatiques et l'appréciation de ceux-ci par les entreprises. Ce fut pour nous l'occasion de constater que les entreprises n'y sont pas assez sensibilisées, la faiblesse de leur budget consacré à la sécurité informatique, entre autres, trahissant leur méconnaissance de la menace constituée par la criminalité informatique.

Cette méconnaissance va bien évidemment permettre à la criminalité informatique de se développer, au sein même de l'entreprise ou à l'extérieur de celle-ci, preuve s'il en est de l'importance d'une politique de prévention efficace tant à l'intérieur qu'à l'extérieur de l'entreprise.

Ensuite, nous nous sommes penchés sur le réseau Internet. Celui-ci étant le vecteur principal des infractions de piratages informatiques, son analyse nous a permis de souligner l'importance de l'aspect de facilité d'apprentissage véhiculé par ce réseau. Apprentissage qui ne se limitera bien souvent pas aux connaissances légales, et qui débouchera souvent sur des activités plus obscures, comme le hacking, ou encore la création de bombes et autres cocktails molotovs.

Cette analyse nous a également permis de mettre en lumière l'aspect international du hacking, celui-ci n'étant désormais plus limité « géographiquement » que par l'imagination des criminels informatiques.

Elle fut enfin l'occasion de souligner, après Durkheim, l'utilité sociale du crime informatique, celui étant, entre autres, générateur d'emplois et de progrès techniques.

Nous nous sommes ensuite trouvés face aux difficultés posées par la notion de « criminalité informatique ». Difficultés quant à la définition de ce concept tout d'abord, mais également quant à l'ampleur du phénomène et à son coût.

Ce fut également l'occasion de pointer l'importance d'une connaissance aussi précise et fiable que possible de ces paramètres, tant sur le plan national que international, ceux-ci étant indispensables à la mise en place de moyens préventifs et répressifs efficaces.

La confrontation de la notion de « respect de la vie privée » aux nouvelles technologie a permis de souligner, s'il en était besoin, qu'outre l'intrusion sur l'ordinateur proprement dit, le piratage informatique était constitutif d'une violation de la vie privée de son utilisateur. L'exemple le plus frappant étant le réseau Echelon, qui peut être considéré, à notre sens, comme le plus grand pirate informatique actuellement en activité.

Il nous fallait alors aborder l'analyse des auteurs de crimes informatiques. L'historique du hacking qui fut dressé permit de mettre à jour les différences existant entre la représentation médiatique et la réalité du monde des hackers. Loin de n'être qu'une gigantesque association de malfaiteurs, la communauté des hackers est constituée de « bons » et de « mauvais » hackers, les hackers « purs » (ou « old school ») et les crackers.

Cette distinction permit également de comprendre les motivations des hackers. Ici aussi, coupant court à tout a priori, il nous fallait pointer que ceux-ci n'ont pas tous l'impression de commettre des actes néfastes pour la société, leur conception du bien et du mal n'étant construite qu'en référence au groupe de hackers auquel ils adhèrent. Mais, que ces actes soient néfastes ou pas, ils n'en demeurent pas moins générateurs de dégâts importants.

Nous avons ensuite appris qu'il n'était pas nécessaire d'être particulièrement doué en informatique pour être un hacker, du moins aux yeux de la société, étant entendu que ce titre n'est décerné que par les autres hackers, une fois un « hack » de légende accompli, en insistant sur le fait que ceux-ci, dans leur majorité, détestent les crackers et leurs activités illégales.

De plus, nous avons vu que la nuisance du fait délictueux était proportionnel avec la facilité avec laquelle il avait été réalisé, facilité consécutive de ce qui vient d'être dit concernant les possibilités offertes par le réseau Internet notamment.

La médiatisation des hackers fut l'occasion de pointer deux éléments.

D'une part, cette médiatisation a été un des éléments décidant le législateur à élaborer la nouvelle loi sur la criminalité informatique.

D'autre part, les hackers sont (quasiment) les seuls criminels rédigeant des traités, des thèses, des manifestes,… sur leur monde, leur culture, leur idéologie.

Les considérations concernant l'idéologie des hackers, leur conception du bien et du mal, les normes adoptées par le groupe, …furent confirmées et expliquées par les théories de Sutherland et Sellin.

Ensuite, l'analyse criminologique permit également de souligner que les motivations des hackers, aussi diverses soient-elles, étaient toutes fondées sur un choix rationnel en fonction des opportunités en présence. Ce fut encore l'occasion de souligner l'importance de la notion de facilité, celle-ci devenant même *créatrice* d'opportunité.

Enfin, la partie sur le phénomène des hackers fut clôturée par une rapide analyse concernant l'arsenal aux mains des hackers, et en particulier de la pratique de l'ingénierie sociale.

Si la théorie des opportunités amenait assez logiquement à envisager la prévention sous l'angle situationnelle, l'ingénierie sociale fut l'occasion de pointer les carences de ce type de prévention en matière informatique, en dehors des défauts « classiques » comme le déplacement de l'activité délictueuse chez des victimes moins, ou pas, protégées.

L'ingénierie sociale est l'élément fondamental justifiant une approche globale et concertée de la prévention, qui ne peut se limiter à des outils techniques. Il est essentiel que chacun ait conscience des risques qu'il encourt, et non des risques qu'il croit encourir, comme nous l'avions pointé dans le début de notre exposé. Cette prise de conscience du risque informatique encouru permettra à elle seule d'élaborer une prévention efficace, qui se devra, à notre sens, d'être situationnelle, mais « améliorée », nettoyée de ses défauts par l'adjonction de l'éducation des jeunes et de la formation du personnel, et d'une manière plus générale, de la sensibilisation de l'ensemble de la société à la criminalité informatique.

L'analyse de la prévention situationnelle, outre les avantages et désavantages qu'elle présente et pour lesquels nous renvoyons à la conclusion qui lui est consacrée, fut enfin pour nous l'occasion de développer les théories économiques du crime, et d'expliquer ainsi le développement des sociétés d'audit et de sécurité informatiques, véritables bénéficiaires des tentatives de prévention en matière de criminalité informatique.

L'Etat, comprenant que la prévention dans cette matière n'était plus de ressort et était devenu le fief quasi-exclusif du secteur privé (se risquant encore ci et là à quelques initiatives comme l'élaboration d'un *guide à destination des utilisateurs d'Internet*), se devait d'intervenir, d'une manière ou d'une autre. C'est ce qu'il fit avec l'adoption de la loi du 28 novembre 2000 relative à la criminalité informatique.

Fruit d'une prise de conscience internationale, de la médiatisation importante d'intrusion de pirates informatiques et du besoin d'adapter un arsenal législatif devenu désuet à l'aube du troisième millénaire, cette loi nouvelle donne une impression mitigée.

Tout d'abord, au chapitre des défauts, le législateur s'est refusé à définir certains concepts informatiques importants, comme la notion de « donnée informatique », de « système informatique » ou encore, pire, de « criminalité informatique » ! Bien qu'il se justifie en disant vouloir rester neutre sur le plan technologique afin que la loi soit toujours adaptée aux progrès techniques à venir, rien ne vient justifier, à notre sens, ces absences.

Cette volonté de « bien faire » a parfois même poussé le législateur à s'octroyer des droits relatifs à des biens et des personnes situés à l'étranger, et ce, en l'absence de toute convention internationale.

Nous pensons que cette violation du respect dû à la vie privée est symptomatique de la volonté du législateur de s'accrocher au dernier garant lui permettant d'assurer sa souveraineté, et partant, sa légitimité, à savoir le domaine de la justice.

Si on analyse cette loi sur un plan non plus seulement juridique, mais criminologique, il nous paraît clair que le législateur a voulu couper court à tout ce qui pouvait entraver son action pénale, et obtenir ainsi la main-mise sur un domaine qui lui échappait jusqu'alors, à savoir l'Internet.

Que ce soit dans les travaux parlementaires, dans les réponses faites aux reproches du Conseil d'Etat ou encore de la Commission de la vie privée (quand il l'a consultée), le législateur répond à tout et justifie tout. Ainsi à titre d'exemple, il justifie l'immixtion dans un état étranger et la violation de la vie privée qui en découle (dans le cadre de la perquisition sur réseau) par le fait que le recours à une commission rogatoire est un procédé trop lourd et trop formaliste. Il « s'excuse » ensuite, en proposant simplement la copie de données, et non plus leur saisie, oubliant de préciser, s'il en était besoin, que la vie privée de la personne dont les données sont copiées est toujours violée, tout comme la souveraineté de l'Etat étranger.

Nous ne cherchons pas ici à dire que l'ensemble des justifications sont inadéquates, ayant d'ailleurs souligné que nous sommes en accord avec certaines d'entre elles même si elles ont fait les frais de diverses critiques (comme ce fut le cas pour la question de la nécessité du dol spécial en matière de hacking externe), mais il n'en reste que la volonté de l'Etat nous semble s'en tenir au discours.

Alors que d'un côté, il justifie ses décisions par la prise de conscience internationale du phénomène, de l'autre, il ne donne pas les moyens matériels et humains nécessaires à l'application efficace des nouvelles dispositions introduites par la loi du 28 novembre 2000, comme en témoignent, entre autres, les considérations soulignées lors de l'analyse empirique de la Computer Crime Unit, section spéciale de la police fédérale chargée de poursuivre les infractions informatiques. Cette analyse fut certes limitée à une seule institution, mais, sans insister sur le fait que l'arriéré judiciaire est une réalité avérée dans notre pays, les enquêteurs que nous y avons rencontrés, nous ont confirmé que les problèmes soulevés étaient présents dans l'ensemble des services judiciaires du pays et ce, encore aujourd'hui.

La réponse à notre question principale est donc à l'heure actuelle négative. Tant que l'Etat n'aura pas pris pleinement conscience de la nécessité de ne pas s'arrêter à des accords de principe et de sensibiliser l'ensemble de la société à ce qu'il considère lui-même comme un fléau majeur, nous ne pensons pas que les moyens préventifs et répressifs présenteront toutes les garanties d'efficacité nécessaires.

En d'autres termes, il devra se donner les moyens d'assurer ses politiques préventive et répressive afin que nous puissions, cette fois, souligner toute la pertinence de celles-ci …

Annexes

- Les faits marquant de l'histoire de la criminalité informatique -

- La loi du 28 novembre 2000 relative à la criminalité informatique -

- Glossaire informatique général -

- Petit glossaire du hack -

- Pourquoi le cyberpunk ? -

- Le manifeste hacker -

- Hackitivismo Declaration -

- Comment devenir un hacker ? -

Les faits marquants de l'histoire de la criminalité informatique

Pour cette partie, notre source principale a été le site de Symantec, leader mondial dans le domaine des logiciels de sécurité, dont l'une des adresses est www.symantec.fr, et qui publie une série d'articles sur l'ensemble des domaines relatifs à l'informatique et à l'utilisation qui peut en être faite.

- **1970 :**

John Draper, le « Captain Crunch », découvre de « nouvelles propriétés » au sifflet offert dans les boîtes de céréales, lui permettant de pirater et de ne plus payer les communications téléphoniques.

Grâce à lui, des milliers de personnes pourront passer et s'échanger des informations, gratuitement, par l'intermédiaire du téléphone.

- **1981 :**

- Ian Murphy, alias « Captain Zero », est officiellement la première personne inculpée pour crime informatique.

- c'est l'année de création du premier virus, « Elk Cloner », développé « pour » les ordinateurs Apple II.

- Les exploits du Captain Zero inspireront le film « Sneakers » (« Les experts »), où une bande de hackers repentis se trouvent confrontés à des agents du FBI corrompus.

- **1983 :**

Le film « War Games » popularise les hackers et leurs capacités.

- **1985 :**

Le premier numéro de « Phrack » est publié. Il s'agit du premier magazine « underground » consacré aux hackers et au piratage informatique.

- **1986 :**

- C'est l'année de création du premier virus informatique PC, « Brain »[614].

- Le Computer Fraud and Abuse Ac test vote par le congrès américain.

- **1987 :**

Le virus « Jerusalem » est détecté. Il s'agit du premier virus capable de détruire des fichiers.

[614] Il a été créé au Pakistan.

- **1988 :**

- Robert Morris lâche sur le réseau Internet le premier ver informatique. Celui-ci infectera plus de 6000 ordinateurs.

- Kevin Mitnick est condamné à un an de prison suite à son intrusion dans les ordinateurs d'une grande société.

- **1989 :**

- Le Cybercriminel « Dark Avenger » crée « Avenger.1808 »

- « WDEF », le premier virus Macintosh fait son apparition.

- On compte environ 30 virus en circulation.

- **1990 :**

Début de la guerre entre les groupes de hackers rivaux, les membres de « Master of Deception » et de « Legion of Doom », qui se terminera par l'arrestation des LoDs.

- **1991 :**

- Le virus «Michelangelo » est découvert. Il est conçu pour détruire les données se trouvant sur les ordinateurs infectés le 6 mars, date de naissance de Michel Ange.

- « Dark Avenger » créé « MtE », un logiciel avec pour fonction de rendre un virus polymorphe, lui permettant ainsi d'adopter 4000 milliards de formes différentes, le(s) rendant ainsi très difficile(s) à détecter.

- « Dark Angel » et «Nowhere Man » créent le premier générateur de virus, permettant ainsi à n'importe qui de créer un virus.

- A la fin de cette année, on compte plus de 1000 virus en circulation.

- **1992 :**

- Création de « Monkey », un virus qui efface le disque dur lorsque l'on tente de le supprimer.

- **1994 :**

- Vladimir Levon subtilise électroniquement 10 millions de dollars à la Citybank, faisant perdre à la banque 10 de ses plus gros clients.

- Mark Abene, alias « Phiber Optik », un des leaders des Masters of Deception, est emprisonné pour avoir détourné des lignes téléphoniques. A sa libération, il sera nommé par le «New York Magazine » dans le Top 100 des personnalités les plus intelligentes de la ville.

Cette nomination est un bon exemple de la fascination que les hackers exercent sur les médias. On n'imagine mal un « simple » braqueur de banque recevoir un titre du même ordre.

• **1995 :**

Recherché par le FBI depuis 7 ans, Mitnick est arrêté en 1995, pour une série de crimes, dont le préjudice total s'élèveraità plus de 80 millions de dollars.

• **1996 :**

« Concept », le premiers macro-virus (il s'agit de virus infectant les documents Word) devient le virus le plus répandu dans le monde.

• **1997 :**

La brigade des mineurs déclenche l'opération « Achille » dans toute la France. Visant les milieux pédophiles, elle aboutira à 55 arrestations et 11 mises en examen.

Cette opération est importante dans l'histoire de la criminalité informatique, car elle a été montée sur base de documents, de contacts, parfois même de preuves, obtenus sur et par le Net, et s'attaquait à une forme de pornographie qui était jusqu'alors « à l'abri » des interventions policières.

• **1998 :**

- Le groupe de hackers «Cult of the Dead Cow» développe «Back Orifice», un cheval de Troie permettant un accès complet (et sans limites de distance) aux ordinateurs infectés[615].

- Création du National Infrastructure Protection Center (NIPC) en vue de lutter contre le cybercrime et le sabotage des infrastructures informatiques américaines.

- Le « Dr. Mudge » et d'autres membres du groupe « L0pht » témoignent anonymement devant le Sénat américain à propos de la vulnérabilité des réseaux électroniques.

• **1999 :**

- La nouvelle version de « *Back Orifice* », « *Back Orifice 2000* », fait son apparition.

- Les hackers Serbes et Kosovar se livrent une guerre électronique, chacun piratant les sites de l'adversaire. Deux hackers Serbes, quantà eux, menacent de s'attaquer à l'OTAN, en représailles à la guerre contre la Serbie.

- En Chine, deux cybercriminels chinois sont condamnés à mort pour avoir piraté une banque et détourné 87000$.

- Le site Web de la Maison Blanche est « tagué » de graffitis rouges.

[615] Tous les détails sont disponibles sur le site-même du groupe, www.cultdeadcow.com.

- **2000 :**

- En février 2000, les serveurs des sociétés symboles de la nouvelle économie (parmi lesquels Yahoo.com, Amazon.com, CNN.com,…), font l'objet d'attaques massives et concertées d' hackers de toute la planète, aboutissant à une paralysie de plusieurs heures, un retentissement médiatique mondial important et à un krach boursier sans précédent des valeurs technologiques.

- En Mai 2000, le virus *« I Love You »* infecte des centaines de milliers d'ordinateurs.

- Lors de l'été 2000, le Congrès DefCon de Las Vegas accueille pour la première fois ouvertement et «officiellement » la police, démontrant ainsi la volonté de ses organisateurs de se cantonner à des activités légales.

- En Octobre 2000, Microsoft, le numéro un mondial de logiciels informatiques, découvre qu'il est visité depuis plusieurs semaines par le ver informatique « QAZ ». Microsoft déclarera que ces intrusions sont « sans conséquence sur les produits qui seront fournis aux clients »[616].

- **En 2001 :**

En décembre 2001, on comptait plus de 70000 virus en circulation.

[616] Microsoft, www.microsoft.com.

Pour des raisons d'économie d'espace mémoire, nous renvoyons le lecteur aux différentes adresses Internet référençant ces textes.

La loi du 28 novembre 2000 relative à la criminalité informatique

Le texte de loi est disponible sur le site du Moniteur Belge, www.moniteur.be

Glossaire informatique général

Ce glossaire fait partie du « Guide à destination des utilisateurs d'Internet » réalisé par le CRID, disponible à l'adresse
http://.mineco.fgov.be/information_society/consumers/consumers_Internetguide/homefr.htm

Petit glossaire du hack

Ce glossaire est issu du site Zataz.com, spécialisé dans l'univers du hacking, des pirates informatiques et de leurs pratiques.

Pourquoi le cyberpunk ?

Ce texte est issu du site http://biblioweb.samizdat.net/ qui regroupe divers textes sur le hacking, la cryptographie, la cyberculture,… écrit pour la plupart par des hackers.
Il a été rédigé par « Phantom Writer » (on ne connaît ni sa véritable identité, ni la date à laquelle ce texte a été rédigé), et traduit de l'anglais par Yves Potin.

Le manifeste du hacker

Ce texte, également connu sous le titre *« La conscience d'un hacker »*, écrit le 8 janvier 1986 par « The Mentor », provient également du site http://biblioweb.samizdat.net/.

Hacktivismo Declaration

Ecrit le 4 juillet 2000 par « Hacktivismo » et les membres du « Cult of the Dead Cow », ce texte est disponible sur le site de ces derniers à l'adresse www.cultdeadcow.com

Comment devenir un hacker ?

Ce texte a été écrit par Eric S. Raymond, expert en matière de hackers, et est disponible sur son site personnel à l'adresse www.tuxedo.org/~esr/

Bibliographie

Ouvrages

• BANCAL, D., *Hackers et pirates sur Internet*, Strasbourg, Desmaret, 2001.

• BARTHOLOMEEUSEN, H., e.a., *Internet sous le regard du droit*, Bruxelles, Editions du jeunes barreau de Bruxelles, 1997.

• BATSELE, D., *La lutte contre le racisme et la xénophobie*, Bruxelles, Némesis, Collection Droit et Justice, 1992, 317 p.

• BEREINS, L., *Fiche d'information concernant l'organisation et le fonctionnement du Féderal Computer Crime Unit et des Computer Crime Units régionaux*, Bruxelles,Direction de la lutte contre la criminalité économique et financière, 10 juillet 2001, p. 2.

• BERENBOOM, A., *Le droit d'auteur*, Bruxelles, Larcier, 1984, 293 p.

• BLANCHARD, P., *Pirates de l'informatique*, Paris, Addison-Wesley France, 1995, p. 145.

• BOSLY, H.D., VANDERMEERSCH, D., *Droit de la procédure pénale*, Brugge, La Charte, 1999.

• BOSLY, H.D., e.a., *La loi du 12 mars 1998 réformant la procédure pénale*, Liège, éd. Collection scientifique de la Faculté de Droit de Liège, CUP, 1998.

• CAILLOIS, R., *Les jeux et les hommes*, Paris, Gallimard, 1967.

• CAMPBELL, D., *Surveillance électronique planétaire*, Paris, Allia, 2001.

• CLUSIF, *Etudes et statistiques sur la sinistralité informatique en France. Année 2000*, mai 2001 (disponible à l'adresse http://www.clusif.asso.fr/fr/production/sinistralite/)

• CHAOS COMPUTER CLUB, *Danger pirates informatiques*, Paris, Plon, 1989.

• CHATELAIN, Y., ROCHE, L., *Hackers ! Le 5e Pouvoir*, Paris, Maxima, 2000.

• CLOUGH, B., MUNGO, P., *La délinquance assistée par ordinateur - La saga des « hackers », nouveaux flibustiers « high tech »*, Paris, Dunod, 1993, 224 p.

• CUSSON, M., *Croissance et décroissance du crime*, Paris, PUF, 1990.

• CUSSON, M., *Le contrôle social du crime*, Paris, PUF, 1983.

• DELMAS-MARTY, M., *Droit pénal des affaires*, 3e éd., t.1, Paris, PUF, 1990.

• DUFRESNE, D., LATRIVE, F., *Pirates et flics du Net*, Paris, Seuil, 2000.

• FRANCHIMONT, M., JACOBS, A., MASSET, A, *Manuel de procédure pénale*, Liège, Collection scientifique de la Faculté de Droit de Liège, 1989.

• SCHMID, G. (Rapporteur), *Document de travail*, Commission temporaire sur le système d'interception Echelon, PE 294.297/6REV, 2001, p. 38

• SCHMID, G. (Rapporteur), *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, Commission temporaire sur le système d'interceptions Echelon*, PE 305.391, 2001, p. 103.

• GASSIN, R., *Précis de criminologie*, Paris, Dalloz, 1994.

• GHERNAOUTI-HELIE, S., *Sécurité Internet, Stratégies et technologies*, Paris, Dunod, 2000.

• GIBSON, W., *Neuromancer*, New York, Ace Science Fiction Books, 1984.

• GLINEUR, P., *Droit et éthique de l'informatique*, Bruxelles, Story scientia, A la rencontre du droit, 1991, p. 180

• GUICHARDAZ, P., LOINTIER, P., ROSE, P., *L'infoguerre. Stratégie de contre-intelligence économique pour les entreprises*, Paris, Dunod, 1999.

• HUITEMA, C., *Et Dieu créa l'Internet…*, Paris, Eyrolles, 1995.

• ICHBIAH, D., *Bill Gates et la saga Microsoft*, Paris, Pocket, 1995.

• KAMINSKY, D., *Auteurs de virus, entreprises, éditeurs d'antivirus : les liaisons dangereuses*, Paris, CLUSIF, Octobre 1998.

• LE DORAN, S., ROSE, Ph., *Cyber-thrillers, 35 histoires vraies de délinquance informatique*, Paris, Albin Michel, 1996.

• LEVY, S., *Hackers : heroes of the Computer Revolution*, New York, Delta, 1984.

• LITTMAN, J., *L'intrus. En ligne avec Kevin Mitnick, le fugitif du cyberspace*, Paris, Grasset, 1997.

• LOINTIER, P., (Sld), *A la poursuite de Dark Avenger. L'affaire des virus au goût bulgare*, Paris, Dunod, 1993.

• MACCOBY, M., *Le joueur*, Paris, InterEditions, 1980.

• MARTIN, D., MARTIN, F-P., *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, Presses Universitaires de France, Coll. Criminalité internationale, 2001, 292 p.

• MARY, P., *Délinquant, délinquance et insécurité. Un demi-siècle de traitement en Belgique*, Bruxelles, Bruylant, 1998, p. 683 et suiv.

• MERTON, R., *Eléments de théorie et de méthode sociologique*, Paris, Plon, 1965.

• MEUNIER, C., « La loi du 28 novembre 2000 relative à la criminalité informatique », Act. dr. des technologies de l'information et de la communication, Formation Permanente CUP, vol. XLV, février 2000, p. 35 à 160.

• Ministères des Affaires économiques, *Guide à destination des utilisateurs d'Internet*, éd. du CRID, avril 2000 (disponible à l'adresse http://.mineco.fgov.be/information_society/consumers/consumers_Internetguide/homefr.htm).

• MONTERO, E (Sld), *Droit des technologies de l'information, regards prospectifs*, Bruxelles, Bruylant, 1999.

• MONTERO, E. (Ed.), *Internet face au droit*, Bruxelles, Story scientia, Cahiers du Centre de Recherches Informatique et Droit, n°12, 1997.

• NEY, J.-P., *Terreurs virtuelles. Les nouvelles menaces à l'aube du XXIe siècle*, Chatou, Carnot, Coll. Ciceron, 1999

• PANSIER, F.-J., JEZ, E., *La criminalité sur l'Internet*, Paris, PUF, Coll. Que sais-je ?, 2000.

• PARKER, D.-B., *Combattre la criminalité informatique*, Paris, Oros, 1985,

• PIPERS, A., *Le respect de la vie privée : vos droits, vos obligations*, Bruxelles, Politeia, 1995, 210 p.

• POULLET, Y., DE TERWANGNE, E., TURNER, P., *Vie privée : nouveaux risques et enjeux*, Bruxelles, Story-scientia, Cahiers du Cahiers du Centre de Recherches Informatique et Droit, n°13, 1997 ;

• POULLET, Y., « Internet et vie privée : entre risques et espoirs », J.T., 2001, pp. 155 à 164.

• RIGAUX, F., *La vie privée : une liberté parmi d'autres ?*, Bruxelles, Larcier, Travaux de la faculté de Droit de Namur, 1992, 317 p.

• ROSE, P., LAMERE, J.-M., *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996.

• ROSE, P., *La criminalité informatique à l'horizon 2005. Analyses prospectives*, Paris, L'Harmattan, 1992.

• ROSE, P., *La criminalité informatique*, Paris, PUF, Coll. Que sais-je, Paris, 1995.

• ROSE, P., LAMERE, J-M., *Menaces sur les autoroutes de l'information*, Paris, L'Harmattan, 1996.

• SELLIN, T., *Culture Conflict and Crime*, New York, Social Science Research Concil, 1938.

• SHIMOMURA, T., MARKOFF, J., *Cybertraque – La chasse au pirate informatique le plus célèbre des Etats-Unis*, Paris, Plon, 1998.

• SIEBER, U., *La délinquance informatique*, Bruxelles, Story scientia, Précis et travaux de la Faculté de droit de Namur, n°9, 1990, p. 5

• STERLING, B., *The Hacker crackdown, Law and Disorder on the Electronic*, New York, Frontier Bantam Books, 1992, p.173.

• STROWEL, A., TRIAILLE, J-P., *Le droit d'auteur, du logiciel au multimédia*, Bruxelles, Story scientia, Cahiers du Centre de Recherches Informatique et Droit, n°11, 1997.

• SUTHERLAND, E., CRESSEY, D., *Principes de criminologies*, Paris, Cujas, 1996.

• TULKENS, F., VAN DE KERCHOVE, M., *Introduction au droit pénal*, Bruxelles, Story Scientia, 1998.

• VAN EECKE, P., C*riminaliteit in cyberspace*, Gand, Mys en Breesch, 1997.

• VANDOORSELAERE, Y., LANGLOIS, P., GOLOVANIVSKY, A., *Chevaliers d'Internet et pirates informatiques*, Paris, Editions n°1, 1999.

• WRIGHT, S., *Une évaluation des techniques de contrôle politique, étude intérimaire STOA*, PE 166.499,1998, pp. 20 et ss.

Articles

• BECKER, G., « Crime and punishment : an economic approach», Journal of political economy, 1968, pp. 169 à 217.

• BECKER, N., « La cryptographie et la confidentialité des données : une question clé… », Rev. Ubiquité, 1998, liv. 1, pp. 47 à 66.

• BEREINS, L., « A la recherche des bits criminels, Enquêtes digitales », Politea, Bruxelles, octobre 1998, n°8, pp. 9 à 12.

• BRACONNIER, F., « Criminalité et sécurité sur les systèmes d'information », Liaisons, décembre 1991, n°305, pp. 10 à 23.

• CASTANY, L., FAUVEL, A., HARDOUIN, J., « La cybercriminalité ou le monde des nouveaux pirates », http://membres.lycos.fr/castany, 1999.

• CLARKE, R.V., « Les technologies de la prévention situationnelle », Cahiers de la sécurité intérieure, 1995, n°21, 3e trimestre, pp. 101 à 113.

• COLLARD, I., « Criminalité informatique en Belgique : hier les ténèbres. Demain…. », Rev. Ubiquité, novembre 98, liv 1, pp. 67 à 78.

• COOK, P-J., « The Demand and Supply of Criminal Opportunities », Crime and Justice, University Press, 1986, vol. 7, pp. 1 à 27.

• COUTU, J-S., « Pirates du cyberespace », Quebec Micro (http://www.quebecmicro.com), janvier 1999.

• CUSSON, M., « L'analyse criminologique et la prévention situationnelle », R.I.C.P.T., vol. XLV, n°2, 1992, pp. 137 à 149.

• CUSSON, M., « La criminologie a-t-elle un avenir ? », R.I.C.P.T., 1998, vol. XLI, n°4, pp. 428 à 436.

• DE ROOS, T., « Het concept-wetsvoorstel computercriminaliteit II », Computerr.(Pays-Bas), 1998/2, p. 55 à 58.

• DE VILLENFAGNE, F., DUSSOLIER, S., « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », Auteurs & Medias, 2001, pp. 60 à 81.

• ERLICH, I., « The Economic Approach to Crime, a preliminary Assessment », Criminology Review Yearbook, Sage Publications, pp. 25-60.

• EUDES, Y., « Au bonheur des pirates », Le Monde, jeudi 26 octobre 2000.

• EUDES, Y., « www.2600.org », Le Monde, 26 janvier 2001.

• EVRARD, S., « La loi du 28 novembre 2000 relative à criminalité informatique », J.T., 2001, pp. 241 à 245.

• GASSIN, R., « Les relations entre la prévention situationnelle et le contrôle de la criminalité », R.I.C.P.T., 1996, n°3, pp. 259 à 271.

• GENOT, V., « La cyberpatrouille », Le Vif/L'Express, 1er mars 2002, p. 24.

• GOGGANS, C., « Hackers aren' the real enemy », Computerworld, 8 juin 1992.

• GOLVERS, L., « L'informatique et la protection de la vie privée », http://www.droit-technologies.org, 11 janvier 2001.

• GRABOSKY, P., « Computer crime in a bordeless world », Annales internationales de criminologie, 2000, vol. XXXVIII, n°1/2, pp. 67 à 92.

• HACKTIVISMO, CULT OF THE DEAD COW, « The Hacktivismo Declaration », www.cultdeadcow.com, 4 juillet 2000.

• HALBERT, D., « Discourses of Danger and The Computer Hacker », The Information Society, 1997, n°13, pp. 361 à 374.

• JENNOTTE, A., « La Net-police tracera chaque internaute », Le Soir, 11 août 2000.

• JORDAN, T., TAYLOR, P., « A sociology of hackers », Sociological Review, nov. 46(4), 1998, pp. 757 à 780.

• KAMGA, O., « L'autorégulation de l'Internet et ses répercussions sur le rapport entre les institutions publiques et les citoyens », http://www.er.uqam.ca/nobel/d364101/regulation.shtml, 31 août 2000 ;

• KUTTY ; F., « L'étendue du droit au silence en procédure pénale », Rev.dr. pén., mars 2000, pp. 309 à 334.

• LABROSSE, D., « Hackers, la cyberculture à ses extrêmes », http://www.er.uqam.ca (Université du Québec à Montréal), 2001.

• LABROSSE, D., « Hackers : un nouveau mode de régulation de la société en réseau », Cybermensuel Archée (http://archee.qc.ca), février 2000.

• LAPASSADE, G., « Qu'est-ce que le cyberpunk ? Littérature et contre-culture », www.ai.univ-paris8.fr/corpus/lapassade/cyberpun.htm, 1993.

• MEUNIER, C., « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », Rev. dr. pén., 2001, pp. 611 à 690.

• MOATTI, J-P., « L'économie de la sécurité, de l'évaluation à la prévention des risques technologiques », La Documentation Française, 1989.

• PATAT, J.-C., « Guides du Net », http://patat.isdnet.net/net/indexbis.html.

• PAYE, J.-C., « La loi relative à la criminalité informatique », Journ. proc., 21 septembre 2001, n°420, pp. 12 à 16.

• PHANTOM WRITER, « Pourquoi le cyberpunk ? », http://biblioweb.samizdat.net/, s.d.

• PRADEL, J., FEUILLARD, C., « Les infractions commises au moyen de l'ordinateur », Rev. dr. pén., 1985, pp. 307 à 332.

• RAYMOND, E., « A brief history of Hackerdom », www.tuxedo.org/~esr/, 1999.

• RAYMOND, E., « How to become an hacker ? », www.tuxedo.org/~esr/, 1999.

• RENSON, B., « Du renforcement de la lutte contre le racisme et la xénophobie : du rêve à la réalité ? », Rev. dr. étr. , 1995, p. 3-13

• RENSON, B., « Le racisme, la loi et l'opinion publique », Rev. dr. pen, 1983, p. 727-753

• RICHARD, E., « Hacker brisé », Libération, mardi 14 mars 2000.

• SABATIER, P ., « Crimes sur le Net », www.liberation.fr, 12 décembre 1997.

• SCHREIBER, W., « La délinquance assistée par ordinateur », R.I.P.C., 1997, 51e année, n°464, pp. 9 à 14.

• SHEA, V., « Netiquette », http://www.albion.com/netiquette/book/index.html, 1994.

• SPREUTELS, J.-P., « Infractions liées à l'informatique en droit belge », Rev. dr. pén., 1985, pp. 357 à 393.

• SPREUTELS, J-P., « Le vol de données informatiques », Rev dr. pén., 1991, pp. 1027 à 1064.

• SZABO, D., « La criminalité d'affaires : aspects criminologiques », L'années sociologique, Presses Universitaires de France, 1981.

• THE MENTOR, « Le manifeste du hacker », http://biblioweb.samizdat.net/, 8 janvier 1986.

• VAN EECKE, P., « Het voorontwerp van wet inzake informaticacriminaliteit », Recente ontwikkelingen in informatica-en télécommunicatierecht, Brugge, éd. die Keure, 1999.

• WOOSLEY, J. , « Why America Spies on its Allies », Washington Post, 17 mars 2000.

• X, « Historique d'Internet », WebEncyclo (http://www.webencyclo.com/dossiers/sponsors/wanadoo/contenu/histoire1.asp), 2002.

• X, « La Belgique légifère en matière de cybercriminalité », Manuel des Services de Police, Actualités en bref n°290, 26 février 2001, p. 6.

• X, « La criminalité informatique coûte des milliards de dollars par an », Journal Le Soir, 13 avril 2002.

• X, « Le commentaire du Clusif à propos de la campagne BSA », Logiciels & Systèmes, 1999, mars 1999, n°36. (consultable à l'adresse http://www.grd-publications.com/art/ls036/ls036058.htm).

• X, « Les bâtisseurs d'Internet », Le Monde Interactif (http://interactif.lemonde.fr/article/0,5611,2860-5259-154682-0,FF.html), s.d.

• X, « Petite histoire d'Internet », Le Monde Interactif (http://interactif.lemonde.fr/article/0,5611,2860-5259-45838-0,FF.html), s.d.

• ZAKON, R., « Hobbes' Internet Timeline v5.6 », http://www.zakon.org/robert/Internet/timeline/, 1er avril 2002.

• ZAJAC, B.-P., « Computer Fraud in college, a case study », Securicom, 1985.

Principaux sites Internet consultés

Nous précisons que les références de sites Internet ne contiendront le plus souvent pas de date précise, ceux-ci étant régulièrement mis à jour.

SITES D'INFORMATIONS

- **ASBL Droit et Nouvelles technologies :** www.droit-technologies.org

- **Echelon On Line**, www.echelon-online.fr.st.

- **IDC**, www.idc.fr.

- **Intelligence stratégique**, www.intelligence-strategique.fr.st.

- **Journal du net**, www.journaldunet.com.

- **Le Monde**, www.weblmi.fr.

- **Le site consacré à la cybercriminalité et réalisé dans le cadre de la conférence NTIC de l'IEP Paris en 2000-2001**, www.ifrance.com/cybercrime.

- **Le site d'informations relatives à l'Internet et aux réseaux**, www.internet.com.

- **Sécurité Internet**, www.2si.org.

- **Strategic road**, www.strategic-road.com

- **The Computer Security Insitute**, www.gocsi.com.

- **Zataz**, www.zataz.com.

SITES DE SOCIÉTÉS

- **Edelweb**, www.edelweb.fr.
- **Freebel :** www.freebel.be.
- **Linux**, www.linux.org.
- **Microsoft**, www.microsoft.fr.
- **Norton**, www.norton.com.
- **PGP**, www.pgp.com.
- **Symantec**, www.symantec.fr.

SITES DE HACKERS

- **®™ark,** ww.rtmark.com.
- **Anarchy**, http://come.to/anarchy.
- **Chaos Computer Club**, www.ccc.de.
- **Cult of the Dead Cow**, www.cultdead.cow.com.
- **DefCon**, www.DefCon.com.
- **EFF**, www.eff.com.
- **Eric Raymond**, www.tuxedo.org/~esr/.
- **Free Kevin**, www.freekevin.com.
- **Legions of Doom**, www.legions.org.
- **Richard Stallman**, www.stallman.org.
- **Site Warez**, http://astalavista.box.sk.

INSTITUTIONS DIVERSES

- **BSA :** www.bsa.com.

- **Centre pour l'égalité des chances et la lutte contre le racisme :** www.antiracisme.be/fr/.

- **Conseil de l'Europe :** www.coe.int.

- **Cybercriminstitut**, www.cybercriminstitut.com.

- **M.A.P.I. :** www.info.fundp.ac.be/~mapi/mapi-fr.html.

- **National Infrastructure Protection Center**, (« Centre de protection des institutions nationales »), www.nipc.gov.

- **PedoWatch :** http://pedowatch.org/.

Table des matières

Tome I

INTRODUCTION **3**

PREMIERE PARTIE - LA CRIMINALITE INFORMATIQUE **6**

TITRE I – LE RISQUE INFORMATIQUE ET LES AUTRES RISQUES **7**

SECTION 1 – L'ACCROISSEMENT DES RISQUES **8**

SECTION 2 - TYPOLOGIES DES RISQUES INFORMATIQUES **9**

A. LES RISQUES NATURELS 11
B. LES RISQUES TECHNIQUES 11
C. LE FACTEUR HUMAIN 12
D. CONCLUSION 13

TITRE II – LE RESEAU INTERNET **17**

SECTION 1 - HISTORIQUE **18**

A. LA NAISSANCE : DU SPOUTNIK A L'UNIVERSITE 18
B. L'OUVERTURE AU PUBLIC : LE WORLD WIDE WEB 21
C. LA DEMOCRATISATION INFORMATIQUE 21
D. INTERNET II : LE RETOUR 25
E. CHRONOLOGIE DES EVENEMENTS 26

SECTION 2 - PRINCIPALES APPLICATIONS **27**

SECTION 3 - INTERNET EN CHIFFRES **28**

SECTION 4 - CADRE JURIDIQUE **31**

A. LE SECRET DES COMMUNICATIONS 31
B. LES PRINCIPES DE DROIT PENAL APPLICABLES 33

SECTION 5 – CONCLUSION **34**

TITRE III – LES CARACTERISTIQUES DE LA CRIMINALITE INFORMATIQUE **35**

SECTION 1 – LA NOTION DE « CRIMINALITE INFORMATIQUE » **36**

A. DEFINITIONS 36
B. SIMILITUDES ET DIFFERENCES ENTRE CRIMINALITE INFORMATIQUE ET CRIMINALITE EN COL BLANC 39

SECTION 2 – L'ETENDUE DU PHENOMENE **41**

A. LES PRINCIPALES SOURCES D'INFORMATION SUR LA CRIMINALITE INFORMATIQUE 41
1) Au niveau national *41*
a) Les statistiques policières 41
b) Sondages et enquêtes 42
c) La Business Software Alliance 43

2) Au niveau international *44*
a) Nécessité d'une recherche criminologique internationale 44
b) Le Cybercriminstitut 45
B. LE CHIFFRE NOIR 47

SECTION 3 – LE COUT DE LA CRIMINALITE INFORMATIQUE 49

SECTION 4 – CONCLUSION 51

TITRE IV – LE RESPECT DE LA VIE PRIVEE CONFRONTE AUX NOUVELLES TECHNOLOGIES 52

SECTION 1 – LE RESPECT DU DROIT A LA VIE PRIVEE 54

A. AU NIVEAU INTERNATIONAL 54
1) La Déclaration universelle des droits de l'homme *54*
2) La Convention européenne des Droits de l'Homme *55*
B. AU NIVEAU NATIONAL 55

SECTION 2 – LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL 56

A. AU NIVEAU INTERNATIONAL 56
B. AU NIVEAU EUROPEEN 58
C. AU NIVEAU NATIONAL 59

SECTION 3 – LE RESEAU « ECHELON » : LA DEMOCRATIE SELON LES ETATS-UNIS 61

A. LE PACTE UKUSA 61
B. LES CARACTERISTIQUES DU RESEAU ECHELON 63
1) Echelon : un cran au-dessus des autres *63*
2) Echelon : qualité filtre *64*
C. LA COMPATIBILITE AVEC LE DROIT FONDAMENTAL AU RESPECT DE LA VIE PRIVEE 66
D. LA SITUATION EN BELGIQUE 69
E. LA BOUCLE EST BOUCLEE : L'ECHELON EUROPEEN 71

SECTION 4 –- CONCLUSION 72

DEUXIÈME PARTIE – LE MONDE DES HACKERS 74

TITRE I – HISTORIQUE DU HACKING 75

SECTION 1 – DE L'ALTAIR AU CAPTAIN CRUNCH 75

SECTION 2 – HACKERS ET PHREAKERS : L'UNION SACRÉE 78

SECTION 3 – LE GLISSEMENT VERS LE CYBERCRIME 80

SECTION 4 – LE CONFLIT DES GÉNÉRATIONS 82

A. LA GÉNÉRATION DES ANNÉES 1960 : LES HACKERS « OLD SCHOOL » 83
B. LES ANNÉES 1980 : LA RIVALITÉ DES HACKERS 84
C. LES ANNÉES 1990 : COMMUNAUTÉS VIRTUELLES ET HACKERS SOLITAIRES 86

SECTION 5 – LES HACKERS QUI ONT FAIT L'HISTOIRE 88

A. LES GOUROUS 88
1) Richard Stallman *88*
2) Denis Ritchie et Ken Thompson *89*
3) Steve Wozniak et Steve Jobs *89*
B. LES CYBERCRIMINELS 90

1) Kevin Poulsen *90*
2) Kevin Mitnick *90*

SECTION 6 – LES FAITS MARQUANTS DE L'HISTOIRE DE LA CRIMINALITÉ INFORMATIQUE 92

CONCLUSION QUANT À L'HISTORIQUE DU HACKING 93

TITRE II – LES CARACTERISTIQUES DES HACKERS 94

SECTION 1 – HACKERS, CRACKERS, LAMERS,… 96

A. LE HACKER 96
1) Les Curious Joe *96*
2) Les Script Kiddies et les Lamers *97*
3) Les Wannabes *98*
4) Les Elites *98*
5) Les Corsaires *99*
B. LE CRACKER 100
C. LE PHREAKER 100
D. LES CYPER PUNKS, LES CRASHERS ET LES AUTRES 100
E. CONCLUSION 101

SECTION 2 – CULTURE, IDEOLOGIE ET ETHIQUE DU HACKER 102

A. LA CULTURE CYBERPUNK ET LE CYBERESPACE 102
B. L'IDEOLOGIE DES HACKERS 104
1) La Temporary Anonymous Zone *105*
2) L'Underground *106*
C. HACKERS ET MEDIAS 107
D. LES HACKERS ET L'ETHIQUE 109
1) La théorie des associations différentielles de Sutherland *110*
2) La notion du Bien et du Mal chez les hackers *111*
3) La théorie des conflits de culture de Sellin *112*

SECTION 3 – PROFILS ET MOTIVATIONS DU HACKER 113

A. FACTEURS CRIMINOGENES 114
B. LE PROFIL-TYPE DU CRIMINEL INFORMATIQUE EXISTE-T-IL ? 115
C. LES MOTIVATIONS DES HACKERS 117
1) La typologie de Donn Parker *117*
2) Les principales motivations des hackers *119*
a) Les motivations liées à l'argent et au profit en général 120
b) Les motivations d'ordre intellectuel : le jeu et le défi 122
c) Les motivations d'ordre politique 125
1°) L'hacktivisme 125
2°) Le cyberterrorisme 126
D. LE CHOIX RATIONNEL DE BECKER ET L'INNOVATEUR DE MERTON 129
E. CONCLUSION 132

CONCLUSION QUANT AUX CARACTERISTIQUES DES HACKERS 133

TITRE III – L'ARSENAL DES HACKERS 135

SECTION 1 - VIRUS, VERS ET TROJANS 135

A. LES GRANDES FAMILLES DE VIRUS 136
1) Les vers *136*
2) Les trojans *137*
3) Les bombes logiques *137*
B. LES CREATEURS DE VIRUS 138

SECTION 2 - L'INGENIERIE SOCIALE 139

Tome II

TROISIEME PARTIE – LES MOYENS DE PREVENTION EN MATIERE DE CRIMINALITE INFORMATIQUE.141

TITRE I – PREVENTION SITUATIONNELLE ET MOYENS TECHNIQUES 142

SECTION 1 – LES OUTILS TECHNIQUES 142

SECTION 2 – LA PREVENTION SITUATIONNELLE.....144

TITRE II – UNE SENSIBILISATION ESSENTIELLE AUX RISQUES 148

SECTION 1 – L'IMPORTANCE DE L'EDUCATION.....149

SECTION 2 – LA SENSIBILISATION INDISPENSABLE DU MONDE DE L'ENTREPRISE.....150

SECTION 3 – LE « GUIDE A DESTINATION DES UTILISATEURS D'INTERNET ».....151

CONCLUSION : LA NOTION DE « SYSTEME DE CRIME » 152

QUATRIEME PARTIE - ANALYSE DE LA LOI DU 28 NOVEMBRE 2000 RELATIVE A LA CRIMINALITE INFORMATIQUE 155

TITRE I – LE DROIT PENAL MATERIEL.....158

SECTION 1 – ORIGINE DE LA LOI.....158

A. LE CONTEXTE INTERNATIONAL 159
1) L'O.C.D.E. 159
2) Le Conseil de l'Europe 160
3) L'Association internationale de droit pénal.....162
4) Le G8 163
5) L'Union européenne 165
B. LES LACUNES DE L'ARSENAL REPRESSIF BELGE EN MATIERE DE CRIMINALITE INFORMATIQUE SPECIFIQUE166

SECTION 2 – ANALYSE DE LA LOI.....168

A. DROIT PENAL GENERAL.....168
1) L'auteur.....168
2) La tentative 168
a) La peine applicable à la tentative 168
b) L'incrimination des actes préparatoires 169
3) La récidive 170
4) La confiscation.....170
5) La localisation des infractions informatiques 170
B. DROIT PENAL SPECIAL 172
1) L'informatique comme moyen.....173
a) La pornographie infantile 173
1°) La législation existante.....173
2°) La législation existante peut-elle s'appliquer au réseau Internet ? 175
3°) Conclusions.....176
b) Racisme et xénophobie.....177
1°) La législation existante.....177

2°) La législation existante peut-elle s'appliquer au réseau Internet ? 177
3°) Conclusions 178
2) L'informatique comme but 179
a) Le faux et l'usage de faux en informatique 181
1°) Base légale 181
2°) Origine du texte et ratio légis 181
3°) Commentaires 182
b) La fraude informatique 184
1°) Base légale 184
2°) Origine du texte et ratio legis 184
3°) Commentaires 185
c) L'accès non autorisé à un système informatique et les infractions voisines (le hacking) 187
1°) Base légale 187
2°) Origine du texte et ratio legis 187
3°) Commentaires 188
- Quant au hacking externe 188
- Quant au hacking interne 190
- Quant aux circonstances aggravantes envisagées par l'article 550bis, §3 nouveau 191
- Quant à la provocation à commettre un hacking (article 550bis, §6) 192
d) Le sabotage 193
1°) Base légale 193
2°) Origine du texte et ratio legis 193
3°) Commentaires 194

TITRE II – LA PROCEDURE PENALE LIEE A LA CRIMINALITE INFORMATIQUE 195

SECTION 1 – ORIGINE DE LA LOI 196

A. LES ENQUETES EN MILIEU INFORMATIQUE ET LE DROIT A LA VIE PRIVEE 196
B. L'INSPIRATION INTERNATIONALE 197

SECTION 2 – ANALYSE DE LA LOI 199

A. LA SAISIE DE DONNEES INFORMATIQUES 199
1) Base légale 199
2) Ratio legis 200
3) Commentaires 201
B. L'EXTENSION DE LA RECHERCHE DANS UN MILIEU INFORMATIQUE 204
1) Base légale 204
2) Ratio legis 205
3) Commentaires 206
C. LA COOPERATION DE TIERS 211
1) Base légale 211
2) Ratio legis 212
3) Commentaires 213
- Quant à la nature de la collaboration 213
- Quant à la compétence 213
- Quant aux modalités de l'obligation de coopération 213
- Quant à la responsabilité pénale de l'Etat 216
- Quant l'article 90quater, §4 nouveau du Code d'instruction criminelle 217
D. L'INTERCEPTION DES TELECOMMUNICATIONS 218
1) Bases légales 218
2) Analyse des nouvelles dispositions 219
a) L'article 11 de la loi nouvelle, complétant l'article 90ter, §2 du Code d'instruction criminelle 219
1°) Ratio legis 219
2°) Commentaires 220
b) L'article 12 de la loi, ajoutant un paragraphe 4 à l'article 90quater du Code d'instruction criminelle 220

c) L'article 13 de la loi, ajoutant un nouvel alinéa entre l'alinéa 4 et l'alinéa S de l'article 90septies du Code d'instruction criminelle....221
4) L'article 14 de la loi nouvelle, complétant l'article 109ter E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques....222
1°) Ratio legis....222
2°) Commentaires quant aux destinataires de l'obligation d'enregistrement et de conservation....222
3°) Commentaires quant à l'objet de l'obligation imposée aux opérateurs et fournisseurs....223
4°) Commentaires quant à la durée de conservation des données d'appel et des données d'identification....224
5°) Commentaires quant aux sanctions pénales....226

TITRE III – L'ACTION POLICIERE : ANALYSE EMPIRIQUE DE LA COMPUTER CRIME UNIT....227

SECTION 1 – HISTORIQUE DE L'INSTITUTION....228

SECTION 2 – ORGANISATION DE L'INSTITUTION....228

SECTION 3 – ANALYSE EMPIRIQUE PROPREMENT DITE....230

A. LES MISSIONS DE LA CCU....230
B. LES PROBLEMES RENCONTRES PAR LA CCU....231
a) Le manque de moyens matériels....231
b) Le manque de formation et de moyens humains....232
c) L'impunité des « gros » hackers et la création d'un cercle vicieux....233
C. L'APPORT DE LA LOI DU 28 NOVEMBRE RELATIVE A LA CRIMINALITE INFORMATIQUE....235

CONCLUSION....236

CONCLUSION SUR LA LOI DU 28 NOVEMBRE 2000 RELATIVE A LA CRIMINALITE INFORMATIQUE....237

CONCLUSION GENERALE....239

ANNEXES....244

BIBLIOGRAPHIE....294

TABLE DES MATIÈRES....307