ESSAI SUR LA NOTION DE CYBERCRIMINALITÉ

Par

Mohamed CHAWKI

Membre du Conseil d'Etat
Doctorant en Droit Pénal de l'Informatique à Lyon III

« La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires »

Colin ROSE

INTRODUCTION

1. Les nouvelles technologies, en particulier l'informatique et la télématique, ont une place importante dans la vie économique, et la quantité de transactions et échanges menés par l'intermédiaire d'Internet[1] est en spectaculaire progression[2]. Si ces nouvelles technologies[3] participent de manière positive au développement de la vie économique, elles présentent aussi de nouveaux moyens de commettre des infractions d'affaires, ce qui fait apparaître des dangers non négligeables, vue l'importance qu'elles ont désormais acquise[4].

De même, les infractions informatiques ont le plus souvent un caractère international, alors que les informations en elles-mêmes sont des données régies par le droit national[5]. Dans cette optique, les flux d'informations parcourant librement les autorités chargées de l'enquête sont, elles, strictement liées par leur compétence territoriale nationale et par le principe de souveraineté[6]. Chaque législateur essaie soit de

---

[1] Le mot « Internet » est composé du préfixe « Inter » qui indique un lien entre deux éléments et le mot « Net » qui est traduit de l'anglais par «réseau». Internet est alors un lien entre deux ou plusieurs réseaux informatiques, «un réseau de réseaux». En fait, il s'agit du plus grand réseau informatique de la planète. Il regroupe une multitude de réseaux régionaux, gouvernementaux et commerciaux. Tous ces réseaux discutent entre eux par le biais du même protocole de communication, TCP/IP (*transmission Control Protocol Over Internet Protocol*). La connexion est effectuée par l'utilisation de lignes, des câbles, et des satellites comme joint des lignes téléphoniques. Contrairement aux appels téléphoniques traditionnels, qui transmettent l'information par le circuit commutation. L'Internet transmet l'information par la « paquet commutation » ; dans ce mode, les communications sont changées aux petits signaux. Apres ils sont envoyés aux paquets de bénéficiaire avec arrivant à leur destination par les routes différentes, la communication est alors reconstruite à la fin du récepteur. Sur ces points voir K. HAFNER : *Where Wizards Stay Up Late : The Origins of the INTERNET* (N.Y., TOUCHSTONE) , [1996] p. 12; J. NAUGHTON: *A Brief History of the Future: From Radio Days to Internet Years in a Lifetime* (N. Y. , WoodStock) , [1999] p. 140; A. BRIGGS: *A Social History of the Media: From Gutenberg to the Internet* (Cambridge, Polity Press) , [2002] pp. 311 et s.; Selon une étude réalisée par l'Aftel (Association française de télématique), la France comptait en 1998 plus d'un million d'utilisateurs d'Internet. Le nombre d'ordinateurs raccordés au réseau mondial est passé de 198 000 ordinateurs en juillet 96 à 321 000 en juillet 97, soit une progression annuelle de 62 %. Au niveau global, l'Internet avait plus de 100.000 million des utilisateurs et accessible par plus de 100 Etats. Voir: *Austin Free-Net volunteer; An Introduction to the Internet*. Disponible sur : <http://www.austinfree.net/> (2/3/2001),
et <http://www.sciences-ouest.org/reseau/f0141025.htm> (6/11/2004).

[2] P. –M. REVERDY: La Matière Pénale Á L'Epreuve Des Nouvelles Technologies (Thèse, Université Toulouse I), [2005], p. 79

[3] On parle souvent de « nouvelles technologies » de l'information et de la Communication (N.T.I.C.) ; Cependant il semble que l'adjectif « nouvelle » doit être abandonné. En effet, en raison de la place qu'occupe l'informatique dans notre vie quotidienne et ce depuis plusieurs années, il semble peu approprié d'employer l'adjectif « nouvelle », même s'il est vrai que l'on se surprend encore à user de cet adjectif pour désigner le continent américain (Nouveau Monde) alors que sa découverte remonte à plusieurs siècles. Voir S. El ZEIN, *op. cit.* p. 153 ; A. TOFFLER : La Troisième Vague (Londres, Casserole), [1981] pp.13 et s.

[4] *Ibid.*

[5] Cité par S. El ZEIN : L'Indispensable Amélioration des Procédures Internationales pour Lutter Contre la Criminalité Liée à la Nouvelle Technologie *in* M.-C. PIATTI : Les Libertés Individuelles A l'Epreuve des Nouvelles Technologies de l'Information (Lyon, Presse Universitaires de Lyon), [2001], p. 153.

[6] Le choix de la loi applicable (la détermination de la compétence à légiférer) est appelé à prendre une grande

se protéger sur son territoire, soit d'abdiquer sa compétence législative face à ces actes illicites, soit d'observer et de légiférer aussi peu que possible, ce qui constituer une solution efficace[7]. Cependant, cette situation est insatisfaisante, car elle plonge les internautes[8] dans un réseau de normes multiples, source d'insécurité juridique[9].

Ainsi, organiser la lutte contre la cybercriminalité, c'est tenir compte de l'ensemble de ces paradoxes. Il est nécessaire de considérer les intérêts de chacun afin de parvenir à un équilibre. Les pays qui, pour lutter contre la cybercriminalité, tentent de restreindre l'usage d'Internet comme moyen pour commettre des infractions, s'opposent aux Internautes qui brandissent l'étendard de la liberté de circulation de l'information au niveau mondial[10].

Afin d'appréhender ce phénomène, il est important d'élaborer une définition pratique de ce qu'est la cybercriminalité. Cependant, cette notion est méconnue, peu ou pas définie, son étendue, ses causes ne sont pas clairement établies[11]. Les raisons sont

---

importance dans le contexte du cyberespace et de l'expansion du droit privé. Même si un tribunal est compétent *in personam et ratione loci*, les règles sur le choix de la loi applicable peuvent exiger que le litige soit tranché par une autre juridiction qui serait compétente *ratione materiae*. Chaque pays possède son propre droit international privé. Les variations qui existent d'un pays à l'autre sont précisément ce qui distingue chaque corpus de règles de droit international privé du droit international public. Il est à noter aussi que Industrie Canada a commandité en juillet 1996 une étude préliminaire sous le titre «l'espace cybernétique n'est pas une terre sans loi» sur la responsabilité liée aux contenus d'information sur Internet des prestataires de services d'Internet (PSI), de babillards électroniques, de groupes de discussion, et d'autres services connexes. L'étude fournit une analyse sur la façon dont s'applique la loi canadienne à la responsabilité liée au contenu d'information sur Internet dans les domaines suivants : droit d'auteur et marques de commerce, vie privée et diffamation, obscénité, pornographie juvénile et littérature haineuse. Elle a conclut que « *la révolution technologie qui présentait divers défis d'application, d'exécution et de respect des lois, et que s'il y aurait des modifications sur les législations actuelles, elles devraient intervenir le moins possible* ». Elle a conclu aussi que « *le législateur devrait mettre en équilibre les intérêts des utilisateurs, d'une part, et d'autre part, ceux des auteurs tout en préservant la liberté d'expression* ». S. El ZEIN, *op. cit.* ; G. SAGHEER : L'Internet et le Droit Pénal (Le Caire, Dar El Nahda El Arabia), [2002] p.50 et s. Sur ces points voir : A. SALAMA: *The Concise in Private International Relations Law* (Le Caire, Dar Al Nahda Al Arabia), [1987] p.230; F. A. RIAD et Al TORJOMAN: *Conflits des Lois* (Le Caire, Dar Al Nahda Al Arabia), [1998] p.134; J. J. Abdel RAHMAN: *Droit International Privé* (Le Caire, Al Alamia Press), [1956] p.535-538; G. GRAINGER : Liberté d'Expression et Réglementation de l'Information dans le Cyberspace : Perspectives et Principes d'une Coopération Internationale dans ce Domaine, dans *Les Dimensions Internationales du Droit du Cyberespace* (Paris, UNESCO – Economica), [2000] ; J. HUET : Le Droit Applicable dans les Réseaux Numériques, dans G. CHATILLON (dir) : Le Droit International de l'Internet (Bruxelles, Bruylant), [2002].

[7] Cité par S. El ZEIN, *op. cit.*, *voir* N. GAUTHRAUD: Internet, le Législateur et le Juge (Paris, Gaz. Pal.), [1996].

[8] Conseil d'Etat : Internet et les Réseaux Numériques (Paris, La Documentation Française), [1998], p. 254. « *L'utilisateur ou intervenant consulte ou échange des informations à partir de son ordinateur qui est connecté au serveur informatique de son fournisseur d'accès à Internet ou par une ligne téléphonique classique ou par un réseau câblé* ». Voir *Ibid*, p. 250. Voir également C. ANDERSON: *Toward A Fair Network Access Rate Policy For Rural Broadband Service Providers* (JCLP), v. 14.1; J. LARRIEU: L'Internationalité et Internet (Lamy Droit des Affaires), [février 2002].

[9] Cité par S. El ZEIN, *op. cit.* voir aussi C. CUTAJAR : La Loi pour la Sécurité Intérieure (Paris, D.), [2003].

[10] Cité par S. El ZEIN, *op. cit.* p. 154.

[11] Selon Messieurs Daniel MARTIN et Frédéric-Paul MARTIN « *le phénomène de la cybercriminalité est actuellement totalement mondial, et la donne est sensiblement différente* ». Et selon M. Colin ROSE, la cybercriminalité est *« la troisième grande menace pour les grandes puissances, après les armes chimiques et*

multiples[12], dont la plus présente est certainement la frilosité vis-à-vis des N.T.I.C[13]. Les personnes concernées n'ont pas de réelles connaissances de la cybercriminalité, soit parce qu'elles considèrent que celle-ci est trop « compliquée » et hésitent à donner des définitions, ou des solutions à un problème qui change de forme rapidement, soit au contraire parce qu'elles la sous-estiment, phénomène classique dans les politiques de sécurité des Etats[14] et des entreprises. Pour ces raisons, notre article s'interroge sur la notion de cette criminalité. Il commence par conceptualiser la cybercriminalité (**Section 1**), puis à faire une distinction entre cette dernière et les criminalités apparentées (**Section 2**).

---

bactériologiques, et le nucléaire ». Voir D. MARTIN et F.-P. MARTIN : Cybercrime (Paris, Press Universitaires), [2001], avant-propos. Voir également l'ouverture de la réunion du G - 8 sur la cybercriminalité à Paris [15 mai 2000], disponible sur :
<http://cyberpolice.free.fr/> (consulté le 03/01/2006) ; L. COSTES : La Conférence du G8 sur la Sécurité et la Confiance dans le Cyberespace : Un Premier Dialogur (Lamy Droit de l'Informatique et des Réseaux), [Bull. act. C) Juin 2000, n° 126, p. 1. ; J. ROWLEY: *E-Business: Principles and Practice* (Palgrave Macmillan), [2002] pp. 234 et s.

[12] En effet une série de facteurs criminogènes sont caractéristiques de la cybercriminalité : (a) Il y a tout d'abord le niveau d'intelligence, d'ingéniosité des cyber-criminels. Il est clair que s'introduire sur un ordinateur à distance 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 ; (b) 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) 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.

[13] Voir *Filipino arrested in Love Bug case* (ST. PETERSBURG TIMES ONLINE), [May 9, 2000], disponible sur <http://www.sptimes.com> (consulté le 5/9/2003).

[14] Au niveau géographique et politique, le Vice Président des Etats-Unis mettait l'accent sur la distinction entre les Etats « info-riches », et les « info-pauvres », soulignant les abîmes en matière d'équipement informatique et de réseaux au sein de la population mondiale, à la fois à l'échelle des Etats-Unis, et à l'échelle mondiale sous l'influence de ceux qui dénonçaient la croissance des ghettos sociaux, du rappel de ce que l'économie artificielle d'Internet était fondée sur le don, ou par les partisans du cybercommunisme. Le Vice Président a déclaré : « *les couches sociales pauvres semblent condamnées à rester hors ligne. L'exclusion du cyberespace aggravera leurs handicaps. L'illettrisme informatique, si l'on peut traduire ainsi* computer illiteracy, *deviendra un obstacle à la recherche d'emploi. Les créations d'emplois s'opèrent de plus en plus dans la cyberéconomie. En tout état de cause, elles se situent très majoritairement dans les services où les gains de productivité sont attendus du passage au « temps réel ». Laisser se développer une exclusion du cyberespace tendra de plus en plus à cristalliser des ghettos sociaux* ». Voir J.M SALMON : Un Monde à Grande Vitesse. Globalisation, Mode d'Emploi (Paris, Seuil), [2000], p. 157.

SECTION I

LE CONCEPT ET L'OBJET DE LA CYBERCRIMINALITÉ

2. Le terme *cybercriminalité* demeure difficile à conceptualiser, car il n'est l'objet d'aucune définition légale (**A**). Ce choix des législateurs a conduit la doctrine à multiplier les définitions de ce terme[15], contribuant ainsi à rendre plus complexes les analyses juridiques. En effet, l'absence de définition légale de ce terme est source de confusions, tant au niveau du domaine de la réflexion, qu'au niveau de l'analyse ou du vocabulaire choisi. Ces confusions nous ont conduit à élaborer une définition pratique (**B**) de ce qu'est la cybercriminalité, afin d'appréhender son phénomène.

A) – L'absence de définition légale de la cybercriminalité

3. La cybercriminalité n'étant pas définie avec rigueur, elle conduit vers des dérives terminologiques. Ainsi, MM. Alterman et Bloch retiennent comme définition du délit informatique, la définition de la cybercriminalité proposée par des experts de l'Organisation pour la Coopération et le Développement Economique (OCDE), à savoir « *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données* »[16]. Ces juristes, intégrant dans leur définition la notion morale, semblent considérer que le droit pénal ne peut à lui seul contenir toute l'approche « sanction » de l'utilisation frauduleuse de l'informatique. Cependant, cette démarche ne saurait être retenue dans la mesure où les chartes de règlement des litiges, telle la charte de l'Internet par exemple, ont révélé leurs limites comme monde alternatif de règlement des conflits. L'application de la norme pénale se pose ainsi comme solution face à l'échec de ces initiatives[17]. La confusion opérée par ces auteurs, entre la cybercriminalité et le délit informatique, s'avère symptomatique d'une difficulté d'appréhender cette forme de délinquance. Ce constat légitime l'approche du Professeur Lucas qui considère que « *la seule démarche acceptable consiste à réserver l'acception de fraude informatique aux hypothèses dans lesquelles la technique informatique est au cœur de l'agissement incriminable* » *tout en*

[15] Voir infra 5 et suivant.
[16] H. ALTERMAN et A. BLOCH : La Fraude Informatique (Paris, Gaz. Palais), [3 sep. 1988] p. 530.
[17] *Ibid.*

sachant fort bien qu'il est parfois difficile d'isoler le « noyau dur » de la « périphérie »[18].

La nécessaire clarification des actes qui relèvent de la cybercriminalité a conduit la doctrine à multiplier les notions désignant les actes illégaux en rapport avec l'informatique. Cette démarche a engendré une pléthore de définitions doctrinales de la cybercriminalité en Europe (**1**) et aux Etats-Unis (**2**).

1. Une pléthore de définitions adoptées en Europe

4. Aucun texte législatif ou réglementaire ne définit la cybercriminalité. Toutefois, certaines notions proches, telles que la criminalité informatique, l'infraction informatique, le délit informatique ou l'usage abusif de l'informatique, ont fait l'objet de définitions posant la question de l'assimilation ou de la distinction du crime et de la cybercriminalité. Selon le ministère de l'Intérieur français, la cybercriminalité recouvre « *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP*[19]*, appelés communément l'Internet*»[20]. Selon l'O.N.U., la « *cybercriminalité* » doit recouvrir « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent* », et dans une acception plus large « *tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique* »[21].

Pour l'Office fédéral de la police suisse, la cybercriminalité s'entend « *des nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information, et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels* »[22]. Enfin, le Collège canadien de police définit la cybercriminalité comme « *la criminalité ayant l'ordinateur* [23] *pour objet ou pour instrument de perpétration principale* »[24].

---

[18] A. LUCAS : Le Droit de l'Informatique (Paris, PUF), [1987] n° 413.

[19] Désigne les protocoles communs de communication utilisés par l'Internet, permettant l'interconnexion généralisée entre réseaux hétérogènes.

[20] Le Ministère de l'Intérieur Français <http://www.interieur.gouv.fr/> (consulté le 24/11/2004).

[21] Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants », [10 – 17 avril 2000], disponible sur <http://www.uncjin.org/> ,(consulté le 12/11/2004).

[22] Rapport d'analyse stratégique, [Octobre 2001].

[23] En effet, la langue française distingue deux mots: l' « informatique » et l' « ordinateur ». En 1965, l'Académie française définissait l'informatique comme « le support des connaissances économiques, sociales et scientifiques

Cependant, ces définitions ne sont pas complètement définitives : la définition adoptée par le ministère de l'Intérieur français vise seulement les infractions dirigées contre les réseaux de télécommunications. Elle ne recouvre ni les infractions susceptibles d'être commises sur les systèmes informatiques, ni les infractions directement générées par le fonctionnement des réseaux informatiques. Il s'agit des infractions portant sur l'information véhiculée par le système informatique comme l'escroquerie, l'abus de confiance, et les atteintes aux libertés individuelles par la création illicite de fichiers nominatifs[25]. De même, la définition proposée par l'O.N.U. utilise le terme *comportement illégal* pour se référer à la cybercriminalité. Cependant, un comportement peut être considéré illégal dans un Etat et légal dans l'autre. Enfin, les deux dernières définitions considérées par l'Office fédéral de la police suisse, et le Collège canadien de police utilisent des termes très larges qui peuvent recouvrir la cybercriminalité, et la criminalité informatique en même temps. Ces confusions nous ont conduit à nous interroger sur quelques définitions adoptées aux Etats-Unis.

---

en particulier pour les machines automatiques. Ces machines sont les ordinateurs, qui traitent l'information dans tous les domaines ». Voir N. BLANQUET : La Protection des Programmes d'Ordinateurs (Mémoire, Paris II), [1979] p. 6 ; N.KHATER: La Protection Juridique du Logiciel Dans le Cadre de la Propriété Intellectuelle Dans les Pays de Langue Arabe (Thèse, Nantes), [1995] p. 2 ; J.-P. GILLI : Le Juriste et l'Ordinateur (Paris, Chron.), [1967] p. 47. Dans le domaine informatique, comme dans d'autres domaines, on distingue différentes générations, le passage de l'une à l'autre étant marqué par un saut technologique. La nouvelle génération est caractérisée par les Robots, disponible sur <http://www.robots.net> (04/11/2004). Ce terme a été utilisé pour la première fois en 1921 par l'auteur Karel Capek (1890 -1938) dans une pièce de théâtre s'appelée (*Rossum's Universal Robots*). L'origine du terme vient du mot *Robota*, qui signifie le travail forcé. Sur ce point voir C. FIEVET : Les Robots (Que sais-je ? Puf) [2001] page 19 et s; V. RICHTER : Les Robots de Karel Capek (Prague, Radio Prague), [Janvier 24, 2004], disponible sur l'adresse : <http://www.radio.cz/fr/> (consulté le 04/11/2004). Il est à noter aussi que l'intelligence artificielle a donné lieu à deux courants de pensée. L'hypothèse forte affirme qu'une machine universelle de Turing dotée d'un programme adéquat serait le siège d'un esprit conscient, comme vous et moi L'hypothèse faible prétend, au contraire que cette voie ne peut mener dans le meilleur des cas qu'à une simulation réaliste. Voir J.C. HEUDIN : La Vie Artificielle (Paris, Hermes), [1994], pp. 177 et s; C.REMY : L'Intelligence Artificielle (Paris, Dunod), [1994] pp.20 et s; E. M. PETRIU, et T. E. WHALEN: *Computer Controlled Human Operators* (IEEE Instrumentation Magazine), [Mai, 2002], disponible sur :
<http://www.discover.uottawa.ca> ; V° aussi : B. MURPHY : *The computer in Society* (Kent, Anthony Blond), [sans date] pp.53-61 ; C. DEVERGIES : L'Impact de l'Utilisation des Technologies de l'information et la Communication, dans l'Entreprise, sur la Vie Personnelle du Salarié (Université Lille II, Mémoire DESS), [2004].

[24] Centre canadien de la statistique juridique, disponible à l'adresse :
<http://collection.nlc-bnc.ca/ > (11/11/2004).

[25] G. ROMAIN : La Délinquance Informatique : Où en Est-on ? (Sécurité Informatique), [Juin 1998], n° 20, p. 1.

2. Une pléthore de définitions adoptées aux Etats-Unis

5. Aux Etats-Unis, la cybercriminalité forme une grande proportion des délits examinés par la police [26] .Son concept diffère d'un Etat à l'autre, et d'un département de police à l'autre. Selon le Département de la justice (*United States Department of Justice*) la cybercriminalité est considérée comme « *une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa perpétration, son investigation, ou ses procédures pénales* »[27]. De son coté, le Code pénal de Californie (section 502), définit une liste d'actes illicites qui tombent sous le coup de la cybercriminalité. Il considère comme cybercriminalité le fait « *d'accéder, ou de permettre intentionnellement l'accès, à tout système ou réseau informatique afin a) de concevoir ou réaliser tout plan ou artifice pour frauder ou extorquer ; b) d'acquérir de l'argent, des biens, ou des services, dans le but de frauder ; c) d'altérer, de détruire, ou d'endommager tout système, réseau, programme, ou données informatiques* »[28]. En revanche, le Code pénal du Texas (section 33.02) va plus loin. Il considère comme cybercriminalité, le fait d'accéder à un ordinateur, à un réseau, ou à un système informatique sans avoir l'autorisation de son maître[29]. La confusion opérée par ces législations, entre la cybercriminalité et la criminalité informatique, s'avère symptomatique d'une difficulté d'appréhender cette forme de délinquance. Ainsi, M. WALL déclare que « *le terme cybercriminalité ne signifie plus qu'un acte illicite qui est d'une façon ou d'une autre relatif à l'ordinateur* »[30].

B) – La proposition d'une définition

6. Les exemples précédents illustrent la difficulté et la complexité de ce phénomène. Tandis que certains définitions proposées sont étroites et insistent sur le fait que la catégorie de cette criminalité doit impliquer une opération extrêmement consommée d'ordinateur dans les circonstances où l'infraction ne pourrait pas être commise, les autres exemples sont larges et impliquent beaucoup d'infractions qui sont déjà classées comme infractions traditionnelles. Or, une définition pratique de la cybercriminalité est nécessaire afin d'appréhender ce phénomène. Cette finalité nous conduit à traiter tour à

[26] E. LAWTA: *Law enforcers report spike in cybercrime* (USAtoday.com). Disponible sur : <http://www.usatoday.com/> (11/11/2004).
[27] *U.S. Department of Justice* <http://www.justice.gov/>.
[28] Code pénal de l'Etat de Californie (section 502).
[29] Code pénal de Texas (section 33.02).
[30] D. WALL: *Crime and the Internet* (N.Y., Routledge), [2001], p. 3.

tour le concept du cyberespace (***1***) ; sa relation avec la délinquance (***2***) ; le domaine de la cybercriminalité (***3***) ; et enfin, nous proposerons une définition pratique pour le but de notre étude (***4***).

1. Le cyberespace : mythe ou réalité ?

7. Le « cyberespace » est le terme forgé par le romancier William Gibson[31] pour décrire un lieu dépourvu de murs au sens concret du terme, voire de dimensions physiques. Dans ce dernier, les données mondiales sont structurées sous la forme d'un support visuel[32] et traversable- économie fluide de l'information centrée sur les électrodes du commerce transnational, qui fournissent une interface neurologique directe[33]. Ce type de cyberespace n'existe pas et ne peut pas exister actuellement. Un tel espace électronique est un monde imaginaire[34]. Dans le monde réel, le cyberespace est où les conversations téléphoniques ordinaires ont lieu, où les courriers électroniques[35]

---

[31] Appelé aussi « infosphère »., il est à noter que le préfixe « *cyber* » que l'on ajoute à un mot existant pour en transposer la réalité dans le cyberespace vient du mot grec « *kubernan* » signifiant « gouverner », mais son sens actuel tire son origine du nom cyberspace, inventé en 1984 par l'auteur américain de science-fiction William GIBSON, dans son livre intitulé « *Neuromancer* ». Dans ses écrits, le « cyberespace » s'agissait d'un espace utopique et abstrait où circule l'information. Voir M. DODGE: *Mapping Cyberspace* (N.Y., Routledge), [2001] p. 1. voir aussi P. TRUDEL : Les Responsabilités dans le Cyberespace *in* T. FUENTES – CAMACHO : Les Dimensions Internationales du Droit du Cyberespace (Paris, Economica), [2000] ; J.BARLOW, un des paroliers de *Grateful dead* et auteur de la « Déclaration d'Indépendance du Cyberespace » a repris cette expression pour designer l'espace créé par les réseaux d'ordinateurs. Voir <http://www.elf.org/barlow/~library.html> (visité le 08/12/2003). Voir aussi T. JORDON : *Cyberpower*. *The Culture and Policies of Cyberspace and the Internet* (Londres, Routledge), [1999], pp. 20-58; B. BENHAMOU: Homo Numericus. Petit Essai de Prospectives pour le Cyberspace [15 mars 2001],
disponible sur <http://www.homo-numericus.net/IMG/_article_PDF/article_60.pdf> (consulté le 03/03/2006).

[32] Nous faisons référence au terme support puisqu'il renvoie au droit de la communication qui constitue le cadre de notre recherche. La classification d'Internet dans la catégorie juridique des supports de communication signifie que l'équilibre entre la liberté d'expression et du droit des personnes sur Internet sert de fil conducteur à notre raisonnement. Mais le cyberespace est plus qu'un support qui serait tout entier résumé par le seul droit de la communication. Il est aussi un espace, ce qu'affirme X. LINANT de BELLEFONDS : « *le réseau des réseaux avec ses bandeaux, ses référencements et tout son appareil à la fois merveilleux et cauteleux d'encerclement des intelligences faibles est proprement ignoré, mais il est vrai que le texte* (i.e. la loi de sécurité financière du 1 août 2003, loi 2003-706, article 87.1.14, JO, 2 août 2003) vise toute publicité quel qu'en soit le support. Mais Internet est-il support ou espace ? Beaucoup comme nous pensent qu'il s'agit d'un espace et non d'un support, ce qui n'est pas une dispute byzantine mais une véritable façon d'interpeller les multiples prescriptions de détails du code de la consommation. Le consommateur internaute pend-il un risque spécifique qui affranchit totalement l'offreur du respect des règles propres à la presse et à la télévision ? Voir G. DECOCQ : Commerce Electronique, Concurrence et Distribution, Question d'Actualité (Com. Com. Electr.), [oct. 2003], pp. 14-19 ; S. BRENNER : *Toward A Criminal Law For Cyberspace : Distributed Security* (B.U.J.SCI. & TECH.L.) ; vol. 10 – 1; voir S. BERHARD: Comment Sécuriser le Réseau : Confiance Mutuelle et Cryptage (RDAI), n° 3, [1998].

[33] UNISCO : Les Dimensions Internationales du Droit du Cyberespace (Paris, Economica), [2000] p. 161 ; voir également A. Serge KABLAN : La Normalisation Technique et Juridique des Contrats Electronqiues. Disponible sur : http://www.forac.ulaval.ca/

[34] UNISCO *Ibid*.

[35] En effet, l'e-mail présente des analogies avec le courrier postal traditionnel, désormais rebaptisé « snail mail » par les internautes, du point de vue du secret qui doit entourer les correspondances. Pour envoyer un message électronique du destinataire, et, grâce à l'utilisation d'un logiciel adéquat, ce message sera acheminé jusqu'à la boite du correspondant. Ce type de communication est donc, rapide et relativement fiable. Bien sur, le degré de

vocaux et les messages électroniques texte sont stockés et échangés. Dans cet espace des graphiques créés par l'ordinateur sont transmis et transformés, le tout sous la forme d'interactions, d'une part entre les innombrables utilisateurs et d'autre part, entre les utilisateurs et l'ordinateur lui-même[36].

Le cyberespace se présente comme un espace indéfini. Un espace virtuel [37] d'ordinateurs tous reliés entre eux grâce à des réseaux qu'explorent les « cybernautes », dont les systèmes nerveux sont directement branchés sur les réseaux grâce à une prise fixée sur leur crâne[38]. Le cyberespace comporte beaucoup de caractéristiques qui prennent de l'importance lorsqu'on envisage la problématique de sa régulation. Il peut être considéré comme une « illusion », c'est « une hallucination consensuelle »[39]. Il peut être considéré aussi comme une réalité, mais une réalité dans « un monde virtuel ». Un monde d'ordinateurs en réseaux de télécommunications, de logiciels et de données informatiques, avec une présence sentie dans un monde physique, c'est donc une « réalité virtuelle »[40].

Le cyberespace est un espace complexe à comprendre[41]. Il est à la fois naturel et artificiel. Naturel car sa source est naturelle : le monde réel. En même temps il est un espace artificiel. Tout d'abord, le langage utilisé est artificiel - celui des mathématiques- en commençant par le codage fondamental (0,1) et en finissant par des équations mathématiques de plus en plus élaborées[42]. Ces équations sont comme le germe d'une infinité d'images dont la plupart n'ont pas de correspondance dans le monde naturel. Le cyberespace est aussi artificiel parce qu'il résulte d'une technologie sophistiquée, mise en oeuvre par l'être humain[43].

---

convivialité est moindre devant un écran d'ordinateur qu'avec un combiné téléphonique, mais les internautes ponctuent leurs messages de ce qu'on appelle les « smiles ».

[36] L. TRIBE : *The Constitution in Cyberspace : Law and Liberty Beyond the Electronic Frontier* , disponible sur: <http://cyborgresources.us/> (consulté le 15/04/2005).

[37] Selon le philosophe Pierre LEVY « *Est virtuelle une entité déterritorialisée, capable d'engendrer plusieurs manifestations concrètes en différents moments et lieux déterminés, sans être pour autant elle-même attachée à un endroit ou à un temps particulier* ». Sur la nature de cyberespace voir <http://www.archipress.org/levy/index.html> (14/11/2004).

[38] P. TRUDEL : Quel Droit pour la Cyber-Presse ? La Régulation de l'Information sur Internet (Paris, Légipresse), [mars 1996] ; voir aussi M. FRISON – ROCHE : Le Droit de la Régulation (Paris, Dalloz), [2001], n° 7, p. 610 ; voir aussi E. BROUSSEAU : L'Autorégulation Nécessite-t-elle un Cadre Institutionnel ? (Revue Economique), [octobre 2001], vol. 52, hors série.

[39] W. GIBSON : *Neuromancien* (Paris, Coll. J'ai lu), [1992] n° 23,25.

[40] UNESCO : Les Dimensions Internationales du Droit du Cyberespace (Paris, Economica), [2000] p. 237.

[41] Voir dans ce sens L. LESSIQ : *Code and Other Laws of Cyberspace* (N.Y., Lessig), [1999] p. 65.

[42] Disponible sur:
Le concept CET <http://www.boson2x.org/article.php3?id_article=69> (consulté le 05/06/2006); voir également D. COSTELLO et S. LIN: *Error Control Coding: Prentice-Hall Computer Applications in Electrical Engineering Series* (Londres, Prentice Hall), [1982].

[43] *Ibid.*

Le cyberespace agit comme un transformateur du réel en imaginaire[44], et du réel en imaginaire. Une véritable transformation, réelle, imaginaire est possible grâce à l'information quantique, par exemple, la substitution de l'argent substantiel (papier) par la monnaie informatique n'est qu'une illustration élémentaire de cette transformation d'une grande généralité[45]. À cet égard, il n'est ni déterminé ni indéterminé, il permet la mise en jeu de la notion de niveau de réalité et de la logique du tiers inclus. Il est potentiellement un espace transculturel, et transnational, c'est donc l'espace du choix humain[46].

Le cyberespace ne résulte pas d'une conception consciente globale, et n'est certainement pas guidé par une idée simple ou un plan. C'est un « réseau » où des idées disparates sont constamment façonnées en de nouvelles fonctions, de nouvelles structures, de nouveaux protocoles qui sont ajoutés au système existant. C'est un système sans principes de base ni formats de conception définis et immuables[47].

Ainsi, nous pouvons affirmer que :

---

[44] B. MURPHY, *op.cit.* pp.53-82; L. SHYLES: *Deciphering Cyberspace: Making the Most of Digital Communication Technology* (Dover, Sage), [2002] p.179; J.PREECE: *Online Communities: Designing Usability and Supporting Sociability* (N. Y., Wiley), [2000] p.345; D. PARREY: Criminalité Informatique (Mémoire, Université Paris II), [2004]; M. BRIAT: La Fraude Informatique: Une Approche de Droit Comparé (R.D. P.C.), [1985], p. 307.

[45] Le concept CET, *précité.*

[46] Voir *Ibid*,cela nous conduit à s'interroger sur l'ouvrage de M. Benedict ANDRESON consacré à l'« *imaginaire national* ». Pour cet auteur, les nations sont des « communautés imaginées », mais imaginées suivant un « style particulier » : *l'imaginaire national*. En proposant de considérer la nation comme une forme de *communauté imaginée*, Anderson entend mettre en évidence le fait que l'identification nationale participe à ces processus d'identifications collectives qui se réfèrent à des groupes abstraits car « *même les membres de la plus petite des nations ne connaîtront jamais la plupart de leurs concitoyens [...] bien que dans l'esprit de chacun vive l'image de leur communion* ». Partant du même constat, on peut être tenté d'opposer à la fiction de la communauté nationale des communautés réelles fondées sur l'inter-connaissance. Benedict Anderson, pour sa part, considère qu' « *au-delà des villages primordiaux où le face-à-face est la règle et encore..., il n'est de communautés qu'imaginées* », tout comme il n'est de sociétés qu'imaginées. Sans doute parler de « sociétés imaginées » paraît moins paradoxal, puisque la notion de *société* est l'expression d'une conception artificialiste du social. En revanche, la notion de « communauté imaginée » est, en quelque sorte, en porte-à-faux avec la représentation traditionnelle de la *communauté* comme la forme d'organisation sociale la plus naturelle qui soit. Cette opposition entre deux modèles idéal-typiques d'organisation sociale, l'un enraciné dans la nature (la *communauté*), l'autre fondamentalement artificiel (la *société*), qui n'est rien d'autre que la réinterprétation de la philosophie antique, traverse l'histoire de la pensée politique occidentale. Voir B. ANDERSON: *Imagined Communities: Reflections on the Origin and Spread of nationalism* (Londres, Verso), [1991] pp. 37 – 46, et 83 – 112.

[47] Voir sur ce point C. HEBRARD : Le Village Virtuel 3D (Mémoire, Montpellier 3), [2000] p. 4 et s ; B. DEFFAINS : Economie et Ordre Juridique de l'Espace Virtuel, dans E. BROUSSEAU, N. CURIEN (dir), Economie de l'Internet (Revue Economique) hors série, [2001] ; voir aussi J. DIONIS Du Séjour, rapport n° 612 fait au nom de la commission des affaires économiques, de l'environnement et du territoire sur le projet de loi (n° 528) pour la confiance dans l'économie numérique. Disponible sur <http://www.assemblee-nat.fr/12/rapports/r0612.asp> (consulté le 03/03/2006) ; A. JOYANDET et P. HERISSON, L'Entrée dans la Société de l'Information, rapport d'information n° 436, mission commune de l'information sur l'entrée dans la société de l'information, septembre 1997. Disponible sur <http://www.senat.fr/rap/r96-436/r96-436.html>

- La révolution des N.T.I.C. a neutralisé l'espace et le temps, en créant un nouvel espace virtuel : le cyberespace[48]. Ce dernier, à son tour, a rendu l'intéraction culturelle et sociale une réalité globale qui constitue une partie intégrale de cultures nationales distinctives.
- Le cyberespace a transformé le rôle Etat-Nation et sa souveraineté[49]. Il a mené à la prolifération des nouveaux acteurs transnationaux et des modèles institutionnels[50] tels que l'*Internet Society* (*ISOC*)[51], *Internet Corporation for Assigned Names and Numbers* (*ICANN*) [52], et l*'Internet Engineering Task Force* (*IETF*)[53].
- Le procédé continu d'interaction culturelle et d'échanges d'informations dans le cyberespace, facilité et accéléré par les tendances contemporaines de la mondialisation[54], a rendu la culture dans un état continu du flux. Les modèles culturels traditionnels sont de plus en plus transformés par le réseau Internet[55].

---

[48] Voir P. GAUTIER : Révolution Internet : Le Dédoublement de l'Ecrit Juridique (Paris, Le Dalloz), [2000], n° 12, p. V ; P. LEVY : Essai Sur la Cyberculture : L'Universel Sans Totalité (Rapport), [sans date] ; Le Temps : Comment l'Intelligence Collective Peut Surgir Sur le Net (Entretien avec Pierre Lévy), [22 février 2001.

[49] Sur le rôle Etat-Nation et sa souveraineté voir J. ABDEL – RAHMAN : *Les Principes de Droit International Privé* (Le Caire, Al Alamia Press), [1956] p.535-538 ; M. FAHMY : *Les Principes de Droit International Privé* (Le Caire, Mo'assassat Al Thaqafa Al Jame'eih), [1978] pp. 512-513 ; E. ABD'ALLAH : *Droit International Privé* (Le Caire, Dar Al Nahda Al Arabia), [1980] pp. 539-542.

[50]« *Tout d'abord, comme la philosophe Hannah Arendt le rappelle dans* L'Impérialisme, *pour le moment, un monde qui serait au dessus des nations n'existe pas. Elle croit cependant à la possibilité d'un gouvernement mondial. Mais c'est pour aussitôt attirer l'attention sur le risque du totalitarisme intégral qu'il comporterait : "Il est tout a fait concevable et même du domaine des possibilités pratiques de la politique, qu'un beau jour, une humanité hautement organisée et mécanisée arrive à conclure le plus démocratiquement du monde – c'est-à-dire à la majorité – qu'une humanité en tant que telle aurait avantage à liquider certaines de ses parties* ». P. QUEAU : Pour une Politique du Cyberespace (Paris, Odile-Jacob), [2000], p. 15.

[51] L'Internet society a été fondée en 1992. Son objectif est la promotion et la coordination d'Internet. Autorité morale et technique, elle réunit les fonds et légalise les processus de standardisation. Elle comptait en 2000 près de 8.000 membres dans 125 pays. Des grandes entreprises mondiales y participent. Elle est organisée en chapitre dans chaque pays. Voir Le Monde Interactif, [28 juin 2000].

[52] Organisation à but non lucratif créée en 1998. Elle a remplacé l'Internet Assigned Numbers, fondée par Jonathan Postel. Elle gère l'unicité et la répartition des noms de domaine. Elle s'apprête à gérer le cœur technique du réseau depuis son absorption de l'Authority Root Server. Elle est composée de 19 membres.
Voir <http://www.icann.com/index.html> (consulté le 12/12/2004).

[53] Il s'agit d'un groupement libéral et informel de bénévoles. Il est supervisé par l'Internet Engineering Steering Group, et par l'Internet architecture Board. Il est responsable de l'évolution des standards Internet Il est divisé en six domaines d'application : *Applications Area, Operations et Management Area, Routing Area, Security Area, Transports Area,* et *Users Services Area*.

[54] P. LEVY, *op. cit.* ; B. STERN : Vers la Mondialisation Juridique ? Les Lois Helms-Burton et d'Amato Kennedy (Paris, RGDIP), [1996], p. 979-1003. En effet, « *La mondialisation, ce n'est pas simplement l'amplification des échanges, c'est la mise en compétition des systèmes économiques et sociaux. Toute la question est de savoir si ce phénomène est de nature à valoriser le système non marchand (culturel) des sociétés ou si au contraire de la prise en compte des systèmes sociaux dans la compétition conduira à considère ceux-ci comme des coûts* ». Z. LAIDI : Malaise dans la Mondialisation (Paris, Textuel), [2001], p. 45-47 ; voir également S. BERGER : Notre Première Mondialisation (Paris, Seuil), [2003] ; L. YAGIL : Internet et les Droits de la Personne (Paris, les Éd du Cerf), [2006] ; Le Temps : Comment l'Intelligence Collective Peut Surgir Sur le Net (Entretien avec Pierre Lévy), [22 février 2001].

[55] Selon M. Gibson, la cyberculture se vit fantastiquement dans le cyberespace « *comme un dépassement des*

- La navigation dans le cyberespace est devenue un nouveau type de navigation. Une navigation dans la profondeur de la nature « virtuelle », en interaction avec les internautes eux-mêmes[56]. Cette navigation peut être considérée comme la source d'un nouveau type d'imaginaire, qui influence la perception et qui par son rôle, alimente cet imaginaire.
- La causalité dans le cyberespace est différente de celle, locale, régissant le niveau macrophysique et de celle, globale, régissant le niveau quantique[57]. La causalité dans le cyberespace est une *causalité en boucle ouverte,* due à l'interface homme-cyberespace-temps. L'être humain découvre en lui-même un nouveau niveau de perception grâce à son interaction avec l'ordinateur, et l'ordinateur affine ses potentialités par l'interaction avec l'être humain[58].

Ainsi, le cyberespace peut apparaître comme un nouveau monde, un continent inconnu à découvrir sans limites restrictives apparentes[59].

---

limites et tout particulièrement des frontières du corps et de la chair qui sont encombrants dans les voyages ». Et selon M. LEMOS la « cyberculture » est la jonction paradoxale entre la technique et la culture. Cette liaison est un des enjeux important de nos sociétés actuelles. Il ne s'agit pas d'une culture « rationalisée » mais plutôt l'appropriation de la technique par la culture. Selon cet auteur la « cyberculture » est un : « *Ensemble d'attitudes nées à partir du mariage entre les technologies informatiques et les médias de communication. Cet ensemble d'attitudes est le produit d'un mouvement socioculturel pour apprivoiser et humaniser les nouvelles technologies* ». Pour le philosophe Pierre LEVY la cyberculture n'est pas la culture des fanatiques d'Internet c'est une transformation profonde de la notion même de culture. Il déclare : « *Et c'est difficilement séparable des autres transformations sociales que nous connaissons depuis 20 à 25 ans: l'urbanisation galopante; la montée du niveau d'éducation; la mondialisation économique; le développement des contacts entre cultures. L'humanité est en train de se rencontrer elle-même. Internet est pour moi une espèce de matérialisation de l'universel sans totalité* », c'est qu'il n'y a pas de centre du réseau, il n'y a pas de sens unique. Chaque fois que vous avez un nouveau noeud dans le réseau, un nouveau site, un nouveau groupe de discussion, un nouvel abonné, vous avez une nouvelle source d'hétérogénéité et de diversité. Depuis dix ans, vous avez de plus en plus de langues, de thèmes abordés, de pays concernés. C'est un processus absolument passionnant à observer ». Cette culture est donc l'union de la culture « poste moderne » et du développement des NTIC. « *L'institutionnalisation se transforme en tribalisme, le contrat en objectifs ponctuels, la positivité en non-finalité et l'utopie en quotidien le plus urgent* ». Sur ces points voir M. GIBSON, *op. cit.* p. 57 ; C. HEBRARD, *précité*, voir aussi sur ce point J. HUET : Quelle Culture dans le Cyber-Espace et quel Droits Intellectuel pour cette Cyber-Culture (Paris, Chron.), [1998] p. 185 ; Le Temps : Comment l'Intelligence Collective Peut Surgir Sur le Net (Entretien avec Pierre Lévy), [22 février 2001] ; C. HEBRARD, *précité*.

[56]

[57] Voir aussi sur la localisation de l'infraction : M. PUECH : Droit Pénal Général (Litec, Paris), [1988], p. 148 et 149 ; Le Temps : Comment l'Intelligence Collective Peut Surgir Sur le Net (Entretien avec Pierre Lévy), [22 février 2001].

[58] Dans cette optique la *United States District Court for the Northen District of California* a déclare le 7 novembre 2001 dans l'arrêt Yahoo que : « *le réseau Internet permet d'offrir toute information, tout produit ou tout service à chaque internaute et de transformer les espaces juridiques nationaux en frontière de papier* ».

[59] Ce nouvel espace d'expression humaine, en devenir de civilité mondiale, est en perpétuel mouvement. Or, ce mouvement erratique comporte un danger. Car justement « *le temps de la réflexion nous est compté* », relève le Conseil d'Etat qui résume avec une précision prospective minutieuse, l'ampleur des défis politiques, sociaux et juridiques lancés par le développement des nouvelle technologies de l'information et de la communication : « *les réseaux numériques transfrontières induisent une modification substantielle des modes de régulation habituels des pouvoirs publics (notamment en ce que) : la réglementation d'origine étatique doit désormais se combiner avec l'autorégulation des acteurs, c'est-à-dire l'intervention de ceux-ci pour délivrer les principes de la règle de droit dans des environnements non prévus par celle-ci et pour agir de façon préventive contre la commission*

2. L'évolution de la délinquance dans le cyberespace

8. Par rapport au cyberespace, nous témoignons d'une véritable métamorphose de l'ensemble du système international. D'une part, la naissance d'un nouveau système juridique qui implique un changement des relations juridiques transnationales[60], et d'autre part, le développement des N.T.I.C. qui à leur tour ont mené à l'apparition de nouveau type de « délinquance » que l'on nomme « informatique ».

Le mot « délinquant » renvoie étymologiquement au terme latin « *delinquere* » signifiant commettre une faute[61]. En droit pénal, le délinquant est défini comme « *l'auteur d'une infraction pénale, qui peut faire l'objet d'une poursuite de ce chef*»[62]. Dans ce sens, le délinquant informatique serait la personne qui commet un délit informatique[63]. Certains auteurs (ROSE et PARKER)[64], écartent la notion de délinquant informatique, au profit de celle de criminel informatique ou de fraudeur informatique. De son coté, M. LUCAS préfère le terme « délinquance informatique » au terme de « fraude informatique », du fait de l'harmonie qui s'opère entre le sens littéral du mot délinquant et son sens juridique[65]. La connaissance de la délinquance informatique demeure très difficile, à cause de son hétérogénéité. Au vu de certaines études effectuées[66], la délinquance informatique se diffère de la délinquance classique, car cette primaire « *se compose de délinquants spécialisés jeunes par hypothèse, considérés comme employés modèles occupant un poste de confiance dans la direction d'une*

---

d'infractions (ensuite en ce que) compte tenu des limites inhérentes à toute initiative purement nationale, la coopération internationale des Etats est nécessaire pour faire respecter l'ordre public dans un espace largement dominé par l'initiative privée. En d'autres termes, Internet et les réseaux introduisent une double indépendance entre acteurs publics et privés et entre Etats eux-mêmes, ce qui rend toute politique en la matière très complexe à élaborer et à mettre en œuvre ». Voir J.-P. MIGNARD, *op. cit*. p. 25.

[60] P. ALLOT : *The Emerging Universal Legal System* (International Law Forum du Droit International), [2001] 3(1), p. 14. ; L. MARTINEZ: *The Emerging International Legal Regime for Cyberspace: Implications for Eastern/ Central Europe* (Caroline du nord, Conférence), [5-10 juin 1996], disponible sur <http://www.csulb.edu/~martinez/ipsa.html > (19/11/2004).

[61] J.-F. CASILE : Le Code Pénal Á L'Epreuve De La Délinquance Informatique (Thèse, Aix-Marseille), [2002], p. 17.

[62] S. GUINCHARD et *alii* : Lexique des Termes Juridiques (Paris, Dalloz), [2001].

[63] J.-F. CASILE, *op. cit.* p. 17.

[64] P. ROSÉ : La Criminalité Informatique (Paris, Collection Que-sais-Je ? PUF), [1987] ; D.-B. PARKER : Combattre la Criminalité Informatique (Paris, OROS), [1985] p. 18 ; J.-F. CASILE, *op. cit.* p. 17.

[65] A. LUCAS : Le Droit de l'Informatique (PUF), [1987] n° 413.

[66] G. CHAMPY : La Fraude Informatique (Thèse, Aix-Marseille), [1990] ; A. FRYDLENDER : La Fraude Informatique, Etude Phénoménologique et Typologique Appliquée au Contexte Français (Thèse, Paris 9), [1985] ; S. JERRAI : La Fraude Informatique (Thèse, Montpellier), [1986].

entreprise. Généralement motivés par le caractère du jeu et du défi qu'apporte l'idée de tromper l'ordinateur »[67].

Pour les auteurs, les délinquants en informatique sont insensibles aux valeurs qui n'ont pas d'incidences matérielles. L'éclatement de la relation binaire « auteur-victime » engendre l'absence de scrupule. Le délinquant en informatique ne bénéficie pas de l'image stéréotypée du délinquant classique, qualifié de respecter par son statut social et son niveau culturel. La délinquance informatique étant peu violente, elle n'épouvante pas les victimes. Dans cette optique, M. ROSE distingue : (a) l'utilisateur qui recherche le profit d'un capital financier ; (b) les destructeurs qui composent une frustration professionnelle ou personnelle et qui ne commettent que dans le but de nuire aux entreprises ou aux organisations ; et (c) l'entrepreneur qui vise l'activité ludique et le défi des agressifs qui compensent une frustration personnelle ou professionnelle[68]. De son coté M. BOLONGA isole quatre types de délinquants : (a) l'utilisateur qui recherche le gain financier ; (b) l'utilisateur qui recherche une reconnaissance sociale ; (c) l'utilisateur qui recherche la perte du sens des réalités ; et enfin (d) l'utilisateur ayant un comportement idéologique, qui veux se venger de la société[69].

Associé au développement de l'ordinateur, le délit informatique ne voit le jour qu'à la fin des années cinquantes[70]. Cependant, le premier délit lié à l'informatique et identifié comme tel puis poursuivi au niveau fédéral, aurait été réalisé en 1966[71]. En France, l'une des premières études relatives à la fraude informatique a été réalisée fin des années soixante-dix par un groupe de travail de l'Association française de normalisation (AFNOR)[72]. Ensuite en 1980, l'Institut des Sciences Criminelles de la Faculté de Droit de Poitiers a publié son étude sous « Le Droit Pénal Spécial Né de l'Informatique ».Dans cette optique, l'on peut considérer la délinquance informatique comme un phénomène récent lié au développement technologique et à l'utilisation des ordinateurs. L'émergence des réseaux informatiques transnationaux a mené à la naissance des pirates informatiques ou des *hackers*[73]. Ce développement de technologie

---

[67] S. JERRAI. *op. cit*. p.18.
[68] P. ROSE : Menaces Sur les Autoroutes de l'Information (Paris, L'Harmattan), [1996] p. 15.
[69] G.-J. BOLOGNA : *An Organizational Perspective on Enhancing Computer Security* (Commuincation au Congres Securicom), *in* D. MARTIN: La Criminalité Informatique (Paris, PUF), [1997] p.68.
[70] K. BEAVER: *Hacking for Dummies* (Canada, Wiley), [2004].
[71] V.GOLUBEV: *Computer Crime Fighting Problems*. Voir egalement M. CLEMENTS: *Virtually Free from Punishement until Proven Guilty: The Internet, Web-Cameras and the Compelling Necessity Standard* (RICHMOND JOLT), vol. XII, Issue 1, [2005].
Disponible sur <http://www.crime-research.org/library/Gol_te.htm> (consulté le 19/11/2004).
[72] AFNOR : Sécurité Informatique, protection de données (Paris, Eyrolles), [1983].
[73] Les *hackers* sont des passionnés d'informatique qui inventent et innovent pour le plaisir, non au service d'une

des télécommunications a substitué la « délinquance informatique » à la « délinquance informationnelle », ou la « criminalité informatique » à la « cybercriminalité ». Cela a permis aux délinquants de sortir du champ d'incrimination des infractions liées à l'informatique et d'entrer dans le champ d'incrimination des infractions liées au cyberespace. Dans ce dernier, les systèmes informatiques correspondent généralement à tous les composants fonctionnels d'un ordinateur[74]. Ils évoluent entre deux éléments : le matériel et le logiciel[75]. Ce dernier traite automatiquement les informations lesquelles sont échangées par les réseaux[76].

Les systèmes informatiques sont tous reliés entre eux grâce aux réseaux de télécommunication[77]. Ces réseaux permettent aux systèmes informatiques de partager les programmes, les données et les matériels périphériques[78]. Dans notre étude, les réseaux de télécommunications seront aussi regroupés dans une catégorie avec les réseaux informatiques. Aujourd'hui, le réseau Internet est un exemple type d'un réseau informatique où les ordinateurs sont connectés et sont capables d'échanger les données entre eux[79]. La généralisation de l'accès à l'informatique de réseau, et notamment à

---

information ou d'une entreprise. Le sens de « pirates informatiques » souvent donné au terme est tendancieux et injustifié. Voir M. CASTELLS: La Galaxie Internet (Paris, Fayard), [2001], p. 10; voir également le *New Hackers Dictionary: Who Enjoys Explorating the Details of Programmatic Systems and How to Stretch their Capabilities*, disponible sur <http://techreview.com/articles/apr95/Roush.html>. Le phénomène est encore perçu comme attractif et inoffensif, notamment par les adolescents du monde entier qui voient en lui une forme d'espièglerie, « *a form of mischief* » , voir S. BIEGEL : *Beyond our Control ? Confronting the Limits of our Legal System in the Age of Cyberspace* (Londres, MIT Press), [2001], p. 63. Voir également B. J. FOX: *Hackers and the US Secret Secrvice*, disponible sur <http://www.gseis.ucla.edu/icpl/hfox.htlm> (consulté le 12/02/2004). Mais sa perception peut changer en fonction de l'appréciation des dangers croissants dans le monde : « *There are growing concerns worldwide regarding the danger of cyberterrorism, cyberattacks and cyberwars* » (S. BIEGEL, *op. cit.* p. 62. Voir aussi N. SHER: *The Weapons of Infowar* (*The Jerusalem Report*), [8 juin 1998]. Cette évolution est sensible dans le discours du Président Clinton. Des initiatives de piratage peuvent être prises pour saboter le réseau électronique américain avec des codes de destruction informatique, afin de paralyser l'infrastructure informatique dont dépendent les réseaux bancaires et financiers : « *Twarting hackers armed with destructive computer codes and terrorists intent (...) We will developp better ways of shaing infomation between public and private sectors so that we better prepare for possible cyber-attacks* » I. BRODIE: Clinton Agenda Targets Terrorist Hackers (Londres, The Times), [20 janvier 1999]; T. HINNEN: *The Cyber – Front in the War on Terrorism; Curbing Terrorist Use of the Internet* (5 COLUM. SCI. & TECH. L. REV.), [15 decembre, 2003]. [Le 26 septembre 2002, les rédacteurs du journal *Hackers Voice* dont le numéro d'octobre avait pour sujet principal une faille de sécurité affectant les sites d'une dizaine de grandes banques françaises ont été interpellés. Ils ont été gardés à vue. Selon le directeur de publication de ce journal, « *Hackers Voice a pour principe de contribuer à donner aux citoyens les moyens de critiquer eux-mêmes, lorsque c'est nécessaire, le fonctionnement des réseaux dont ils sont clients et utilisateurs (...) mais notre alarmisme dessert peut-être l'information que nous voulons faire passer* », C. SPINELLI : Des Hackers Citoyens Passent une Nuit en Garde à Vue (Paris, le Monde), [3 octobre 2002].

[74] M. SMITH et P. KOLLOCK: *Communities in Cyberspace* (N.Y, Routledge), [1999].

[75] R. WHITE et T. DOWNS: *How Computers Work* (Corporation), [2002].

[76] *Ibid*.

[77] A. TANEBAUM: *Computer Networks* (N.Y, PH, PTR), [2003].

[78] Dictionnaire Encyclopédique Bilingue de la Micro-informatique (Microsoft), [1998] p.46 ; J. HILDEBERT : Dictionnaire Français – Anglais Anglais Français de l'Informatique (Paris, Pocket), [2004].

[79] La technologie avait imprimé sa marque, son rythme et l'ampleur de l'invention. En huit ans et demi

l'Internet, a uniformisé les différentes formes de délinquance informatique du fait de deux critères constants, à savoir le caractère transnational de l'infraction et l'atteinte à l'information. Par conséquent, la probable utilisation des systèmes informatiques par la délinquance traditionnelle, et la probable mutation de la « délinquance informatique » en une « délinquance de l'information », laisse supposer que la « délinquance traditionnelle » deviendra « informatique » par les moyens qu'elle utilisera. À cet égard, on peut identifier une grande variété d'agissements délictueux au sein du cyberespace. Il est, d'une part, devenu le vecteur d'un certain nombre d'infractions « classiques » tout en amplifiant leur portée (**a**), et d'autre part, il est l'objet d'infractions dites informatiques(**b**).

a) Le cyberespace: instrument actif qui favorise la commission de l'infraction

9.Compte tenu de l'éventail des nouvelles technologies mises à la disposition des personnes malveillantes et qui font une large place à l'ingéniosité d'une part et de la spécificité des délits informatiques d'autre part, l'usage des N.T.I.C pour commettre des nouvelles infractions est devenu un phénomène international. Internet a fait fleurir une multitude d'infractions liées à la circulation de l'information telle que les violations du droit d'auteur[80] , les violations de vie privée et du secret des correspondances[81], les délits de presse et de diffamation[82], etc[83].

---

d'existence, le « *backbone* » était passé d'une capacité de 6 nœuds avec 56 kps à la connexion à 21 nœuds avec 45 Mbps. L'Internet était désormais constitué de 50.000 réseaux locaux sur les cinq continents, dont environ 29.000 aux seuls Etats-Unis. Il était devenu un réseau transfrontière. Le nombre d'utilisateurs d'Internet pouvait être évalué entre 80 et 100 millions d'Internautes en 1998 contre un millier seulement en 1990. En 1996, le trafic sur Internet s'est accru de 30% par mois, 85.000 noms de domaines ayant été mensuellement enregistrés. Grâce à l'efficacité de la recherche et aux moyens mis en œuvre (environ 200 millions de dollars entre 1986 et 1995), la qualité des protocoles développes sur Internet ne faisait plus débat, et lorsqu'en 1990, le réseau APRANET fut définitivement démantelé, le protocole TCP/IP avait définitivement supplanté, ou tout au moins marginalisé, toutes les autres initiatives mondiales. La maturité technique d'Internet, le succès du Web qui commençait à se profiler, ainsi que l'ouverture des réseaux aux services commerciaux et à la concurrence, constituent les ingrédients fondamentaux de la recette d'Internet auprès du grand public. C'est cette mutation qui a conduit les instances normatives à l'échelon et international à s'en saisir. Voir Conseil d'Etat : Internet et les Réseaux Numériques, *op. cit.* ; L. COHEN-TANUGI: Le Nouvel Ordre Numérique (Paris, Odile-Jacob), [1999], p. 150.

[80] TGI Paris : [14 août 1996], (*D.*), [1996], p. 490, note P.-Y. GAUTHIER. La jurisprudence française s'est refusée à considérer que le « *homepage* » d'un délinquant constituait un « domicile virtuel » protégé par l'intimité de la vie privée. Dans la mesure où il y a mise à disposition du public, par un procédé de communication, de signes, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée, il s'agit d'une communication audiovisuelle.

[81] TGI Privas : [3 septembre 1997], (Expertises), n° 213, p. 79 note du Professeur J. FRAYSSINET.

[82] S. JASSERME : La Diffamation sur Internet : Aspects Spécifiques au Réseau (Memoire de DESS, Université Paris II), [2001], voir aussi J.-M. DETAILLEUR, L'Evolution de la presse écrite dans la perspective des nouvelles technologies multimédias, rapport au ministre de la communication, 15 décembre 1994, Légicom, n°8, 1995.

[83] Voir dans cette optique Cass. crim. [17 janvier 2006], (http://www.foruminternet.org), (consulté le

La pédophilie est un exemple particulièrement saisissant de criminalité ayant pris de l'ampleur grâce au cyberespace[84]. Les pédophiles peuvent reproduire des informations ou des photos, l'anonymat y est préservé, la distribution de documents est simple et la quantité de matériaux que l'Internet peut transporter est sans limites. Le cyberespace sert aussi pour la diffusion d'œuvres protégées par le droit de la propriété intellectuelle, et donc la contrefaçon et le marché de copies illicites dans le domaine de la musique, de la vidéo et des logiciels[85]. L'émergence des systèmes d'échanges de fichiers sur le réseau Internet, le développement de sites pirates et la démocratisation des graveurs facilitent ces actes illicites. Dans une affaire, le Tribunal de Grande Instance de Nanterre a condamné pour proxénétisme un individu qui diffusait des messages sur le réseau Internet afin d'attirer des clients potentiels au bénéfice d'une personne se livrant à la prostitution[86]. Aussi, le piratage sur le réseau Internet peut même impliquer des ordinateurs sans que les propriétaires de ceux-ci ne s'en aperçoivent[87]. Le piratage qui, auparavant, nécessitait la compréhension de codes informatiques complexes, est désormais l'affaire d'un simple clic de souris. Selon de récentes estimations, près de 220 millions d'européens dont 22 millions de français disposent d'un accès à Internet, ouvrant ainsi aux pirates informatiques un « marché » en pleine expansion[88].

Selon l'étude réalisée par *Business Software Alliance (BSA)* le 7 juillet 2004 sur les taux de piratage de logiciels dans le monde en 2003, cette infraction atteint un taux de 37% dans l'Union Européenne. Son coût pour les éditeurs nationaux et internationaux a également été chiffré puisque la valeur des logiciels piratés dépasse 9,7 milliards de dollars. L'étude a montré aussi que 45% des logiciels utilisés par les entreprises étaient piratés[89]. Pourtant, les tribunaux n'hésitent plus à condamner durement les contrevenants. Le 13 février 2002, le Tribunal de grande instance de Paris a condamné le créateur d'un site web à payer 15 000 € de dommages et intérêts à l'Agence France Presse (AFP) et à ses journalistes pour la reproduction de leurs photographies. Dans l'espèce, le site *francefun.com* avait reproduit cinq photographies protégées dans une base de données de l'AFP intitulée « Image Forum », et dont l'accès était réservé aux

---

03/03/2006).

[84] S. El ZEIN, *op. cit.* p. 159.

[85] *Ibid* et voir aussi C. KUNER: *European Data Privacy Law and Online Business* (N.Y, Oxford University Press), [2003], p. 39.

[86] TGI Nanterre, 12ème ch., [18 mai 2000], Ministère public c. Jacques L., Comm. Com. Electr. [Novembre 2000], p. 21. Commentaire de Jean Christophe GALLOUX.

[87] S. EL ZEIN, *op. cit.*

[88] *Ibid*, p. 158.

[89] Voir BSA [7 juillet 2004], disponible à l'adresse : <http://www.bsa.org/france/> (19/11/2004).

abonnés détenteurs d'un code confidentiel. Les clichés illustraient des évènements dramatiques de l'actualité et étaient accompagnés, sur le site litigieux, de légendes relevant de l'humour noir. L'agence avait estimé que la reproduction des images portait atteinte aux droits patrimoniaux et moraux des photographes (articles L. 122-4 et L. 121-1 du Code de la propriété intellectuelle). De son côté, le créateur du site invoquait l'exception de parodie et de caricature accordée, lorsque l'oeuvre a été divulguée, par l'article L. 122-5 du Code de la propriété intellectuelle.

Le Tribunal a déclaré dans son jugement que la contrefaçon était bien établie au motif principal que :

> « Les photographies en cause ont été largement diffusées dans le cadre de reportages relatifs à des faits marquants de l'actualité (…) ; que leur reproduction pure et simple, que la légère altération de leur contour ne vient pas atténuer, ne permet pas d'éviter le risque de confusion avec l'œuvre première alors que celle-ci, intacte, demeure chargée de son sens premier nonobstant les légendes qui peuvent y être associées »[90].

De même, le 20 janvier 2004 la Cour d'appel de Douai a entièrement confirmé un jugement rendu par le Tribunal de Grande Instance de Lille, qui avait déclaré la société NDI (RCS de Roubaix Tourcoing) en liquidation, et M. Luc Olivier Lefebvre, gérant, coupable des délits de contrefaçon de marque, de contrefaçon de logiciels, ainsi que du délit de tromperie[91]. Il s'agissait d'une affaire d'exportation et de reconditionnement de produits Microsoft, depuis le marché canadien en violation des termes des licences. M. Luc Olivier Lefebvre a été condamné à une peine de 8 mois d'emprisonnement avec sursis, ainsi qu'à une amende de 3 000 euros[92]. La société NDI a été condamnée à une amende de 5000 euros. Enfin, la Cour a confirmé la condamnation à payer à Microsoft Corporation la somme de 100000 euros à titre de dommages et intérêts[93]. Enfin, un internaute a été condamné au printemps 2005 par le tribunal de grande instance de Paris pour avoir mis à disposition quelque 2 288 bandes dessinées sur Internet[94]. Il a été condamné à verser au Syndicat national de l'édition un euro symbolique au titre de réparation du préjudice subi par l'ensemble de la profession. Le jugement est définitif, l'homme ayant renoncé à faire appel de cette décision.

---

[90] « Condamnation d'un Site Pour Contrefaçon de Photographies de l'AFP », [5 mai 2002], disponible sur <http://www.foruminternet.org/ > (19/11/2004).
[91] Voir : Microsoft France disponible à l'adresse suivante :
<http://www.microsoft.com/>. (12/11/2004).
[92] *Ibid.*
[93] *Ibid.*
[94] Disponible sur <http://www.01net.com> (consulté le 03/03/2006).

b) Le cyberespace: instrument passif favorisant la perpétration de l'infraction

10. Le cyberespace apparaît comme un objet de l'infraction ou comme un instrument passif et l'infraction résulte de ce que le bénéficiaire des informations fournies par le cyberespace ou de la présentation qui résulte de son fonctionnement est sans droit pour les obtenir. Dès lors, il est possible de se trouver confronté à deux hypothèses : dans la première, les informations contenues dans les ordinateurs seront utilisées de façon illicite, alors que la seconde hypothèse concernera le cas de l'utilisation abusive de cet espace virtuel. Des cas concernant la destruction d'ordinateurs, ainsi que des données ou des programmes qu'ils contenaient. Dans cette optique le Tribunal de Grande Instance de Paris a considéré le fait d'accéder au réseau cartes France Télécoms où un individu avait utilisé des numéros d'une carte appartenant à autrui afin d' obtenir des services de télécommunication, comme un fait qui tombe sous l'accès illicite aux systèmes [95]. De même, se rend coupable d'accès frauduleux à un S.T.A.D., ainsi que d'introduction frauduleuse de données dans ce même système, celui qui met en œuvre un programme « sniffer »[96] à l'intérieur d'un serveur connecté au réseau Internet[97].

De même, il était reproché à quatre étudiants de s'être introduits frauduleusement sur le serveur de leur université et d'avoir créé et diffusé des logiciels malveillants[98]. Dès lors que l'intrusion sur le serveur n'a pas été faite sous la surveillance d'un enseignant mais en violation de la charte informatique signée par les étudiants, l'accès frauduleux a été caractérisé. Une amende avec sursis a été prononcée. En revanche, pour les poursuites contre les logiciels malveillants, le mandement de citation au visa du nouvel article 323-3-1 du code pénal a été annulé : les faits reprochés n'étaient pas précisés dans la citation[99].

3. Le domaine de la cybercriminalité

11. L'adjonction de préfixe « *cyber* » qui a tendance à apparaître de manière excessive à chaque utilisation d'un concept classique à l'Internet, à la « criminalité », permet de

---

[95] TGI Paris - 12 ème Chambre [26 juin 1995], (L.P.A), [1 mars 1996] p. 4 n° 27 note Alvarez.

[96] Le « sniffing » consiste à introduire, au niveau d'un serveur par lequel transitent de nombreuses données, un programme informatique spécifique, qualifié de renifleur qui a pour fonction de capturer des données. L'introduction d'un tel programme suppose donc, préalablement, d'acceder frauduleusement à un système de traitement automatisé de données, ainsi que d'y introduire de nouveau éléments logiques, ce qui constitue les délits réprimés par les articles 323-1, al. 1 et 323-3 du Code pénal.

[97] TGI Paris 1e ch. 16 décembre 1997 *in* A. BENSOUSSAN et Y. BREBAN : Les Arrêts Tendances de l'Internet (Paris, Hermès), [2000], p. 45.

[98] TGI Vannes, ch. correctionnelle, 13 juillet 2005, Min. public et Université de Bretagne Sud c. divers étudiants, jugement 1148, 2005. Disponible sur <http://www.droit-technologie.org/4_1.asp?jurisprudence_id=206> (consulté le 03/03/2006).

[99] *Ibid.*

retenir deux sortes de relations entre la criminalité et les réseaux de télécommunications[100]. Dans un premier temps, la criminalité peut être en relation directe avec un réseau de télécommunication, c'est-à-dire que la loi incrimine directement un acte qui, si le réseau de télécommunication n'existait pas, l'acte ne pourrait pas être réalisé. On pense en l'espèce au piratage des réseaux téléphoniques pour effectuer des appels téléphoniques gratuits [101] .

Dans un second temps, la criminalité peut être en relation indirecte avec un réseau de télécommunication, c'est-à-dire que le réseau de télécommunication se comprend comme un outil ou un moyen pour commettre l'infraction[102]. On pense par exemple à l'accès illicite à un système informatique, ou à l'envoi des virus via le réseau Internet. La cybercriminalité au sens strict du terme s'entend donc de l'ensemble des infractions commises contre ou par un système informatique effectué à travers un réseau de télécommunication.[103] Elle requiert obligatoirement l'intervention directe ou indirecte d'un réseau de télécommunication pour commettre l'infraction[104]. Tous les actes perpétrés contre l'assurance de la confidentialité, de l'intégrité, ou de la disponibilité des données ou des opérations de traitement, sont commis dans un environnement électronique impliquant un réseau de télécommunication sont considérés comme une cybercriminalité[105]. Maintenant la plupart des ordinateurs - et par la nature même de la cybercriminalité - tous les ordinateurs qui sont impliqués dans ce genre d'infractions sont connectés à un réseau de télécommunication lequel peut être un réseau local, global ou les deux ensembles.

4. La définition proposée

12. La cybercriminalité peut être définie comme : toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite[106].

---

[100] Voir Office L.F. Quebec, disponible sur : <http://brunosi1.free.fr/terminologie/pages/txtcyber.htm> (consulté le 12/01/2006).
[101] A. BENSOUSSAN : Les Télécoms et le Droit (Paris, Hermes), [1996] pp. 447-483.
[102] *Ibid* p 484 et s.
[103] J.-F. LE COQ : La Cybercriminalité (Mémoire D.E.A., Montesquieu Bordeaux IV), [2002] p. 8.
[104] D.SHINDER: *The Scene of the Cybercrime* (SYNGRESS), [2002] p. 94.
[105] Voir dans ce sens la définition proposée par le ministère de l'intérieur français, *précité.*
[106] La notion d'interconnexion est au cœur du processus d'ouverture à la concurrence des services de communications électroniques. Pour être effective, une telle concurrence doit impérativement passer par un accès à tout réseau ouvert au public. La directive 2002/19/CE du 7 mars 2002 fixe donc deux principes fondamentaux au régime de l'accès et de l'interconnexion, qui font la matière des deux premiers paragraphes de l'article L. 34-8 du CPCE : l'interconnexion ou l'accès d'une part, les exploitants de réseaux ouverts au public

Sous cette définition, nous pouvons identifier les quatre rôles que joue le système informatique dans les actes illicites :

- ***Objet*** : Des cas concernant la destruction de systèmes informatiques, ainsi que des données ou des programmes qu'ils contenaient, ou encore la destruction d'appareils fournissant l'air climatisé, l'électricité, permettant aux ordinateurs de fonctionner.
- ***Support*** : Un système informatique peut être le lieu ou le support d'une infraction, ou un ordinateur peut être la source ou la raison d'être de certaines formes et sortes d'avoirs qui peuvent être manipulés sans autorisation.
- ***Outil*** : Certains types et certaines méthodes d'infraction sont complexes pour nécessiter l'utilisation d'un système informatique comme instrument. Un système informatique peut être utilisé de manière active comme dans le balayage automatique de codes téléphonique afin de déterminer les bonnes combinaisons qui peuvent être utilisées plus tard pour se servir du système téléphonique sans autorisation.
- ***Symbole*** : Un système informatique peut être utilisé comme symbole pour menacer ou tromper. Comme, par exemple, une publicité mensongère de services non existants, comme cela a été fait par plusieurs clubs de rencontres informatisés.

d'autre part. L'interconnexion ou l'accès font l'objet d'une convention de droit privé entre les parties concernées, convention qui est communiquée à l'ART (CPCE et T. art. L. 34-8-1).

SECTION II

LA DISTINCTION DE LA CYBERCRIMINALITÉ ET LES CRIMINALITÉS APPARTENTÉES

13. Les tentatives de définition de la cybercriminalité, ont montré comment ce phénomène est vaste , complexe et touche beaucoup de domaines. Certains auteurs désignant les délinquants, ou qualifiant les actes qu'ils réalisent, commettent parfois des confusions de sens, en désignant sous la terminologie de « *pirate* » tous les délinquants en informatique[107]. Ainsi, il convient d'aborder dans cette partie la distinction de la cybercriminalité et les criminalités apparentées. Il s'agit d'une distinction relative aux termes juridiques (**A**), et d'une distinction relative aux auteurs de l'infraction (**B**).

A) – La distinction relative aux termes juridiques

14. Dans la présente communication, la cybercriminalité est entendue dans un sens large comme désignant toute infraction qui, d'une manière ou d'une autre, implique l'utilisation des technologies informatiques. De même, les notions de « criminalité informatique », « délinquance informatique », « criminalité de haute technologie » sont souvent employées indifféremment. Notre étude établira une destination entre la cybercriminalité et la criminalité informatique (**1**), la criminalité en col bloc (**2**), et la criminalité de haute technologie (**3**).

1. La cybercriminalité et la criminalité informatique

15. Bien que les notions de « criminalité informatique » et de « cybercriminalité » sont étroitement liées, il existe néanmoins une distinction entre les deux conceptions[108]. Ainsi, la criminalité informatique représente l'infraction générique, dont la cybercriminalité est une variante[109]. Cette dernière est une forme particulière de la criminalité informatique, forme qui ne s'exprime que sur et à travers le réseau de

[107] P. BLANCHARD: Pirates de l'Informatique, Enquête sur les Hackers Français (Addison Wesley), [1995].
[108] P. DELEPELEERE: Hackers, l'Autre Monde (Mémoire), [2001 – 2002].
[109] *Ibid.*

télécommunication, contrairement aux autres délits informatiques qui ne nécessitent pas d'intéraction avec le réseau de télécommunication[110].

La complexité de ce type de criminalité s'est alors présentée, les différents auteurs utilisant chacun sa propre définition. Collard fait d'ailleurs remarquer qu'aucune définition n'est acceptée de manière générale[111]. Ainsi, quelques auteurs ont proposé leurs définitions en visant l'ordinateur comme moyen de commettre l'infraction. Selon M. TIDEMANN, la criminalité informatique recouvre « *tout acte illégal commis par ordinateur* »[112]. Selon Mme. L.D. BALL la criminalité informatique est *« une action illicite où l'ordinateur joue un rôle principal pour la commettre* »[113]. Pour MM. R. TOTTY et A. HARDCASTLE la criminalité informatique recouvre « *les infractions liées à l'ordinateur comme un instrument positif plus que négatif* »[114]. Chez M. COMER « *la mauvaise foi financière qui utilise l'environnement informatique est une fraude informatique* »[115]. Pour M. Parker, la criminalité informatique est « *tout acte illicite nécessitant une connaissance spécialisée de l'informatique, au stade de la perpétration, de l'enquête de police ou des poursuites pénales* ».[116] De son coté, Monsieur D. MARTIN propose comme définition : « *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* »[117].

[110] Voir P. DELEPELEERE, *op. cit.*; E. CESAY: *Digital Evidence and Computer Crime* (Londres, Academic Press), [2000] pp.9 et s.
[111] *Ibid.*
[112] K. TIEDEMANN : Fraude et Autres Délits d'Affaires Commis à l'Aide d'Ordinateurs : (Bruxelles, Rev. D.C.P.), [1984], n° 7, p. 612.
[113] L. D. BALL: *Computer Crime* in *The Information Technology Revolution* T. FORESTER (Cambridge, MIT Press), [1985] pp. 543-544.
[114] R. TOTTY, et A. HARDCASTLE: *Computer Related Crimes* (Londres, Macmillan), [1986] p. 169.
[115] M. J COMER: Corporate Fraud (Londres: McGraw-Hill), [1985] p.141.
[116] D.-B. PARKER : Combattre la Criminalité Informatique. *op.cit*. p. 18.
[117] D. Martin, et F.-P. MARTIN, *op. cit.* p. 13.

Quelques auteurs ont proposé des définitions en visant l'ordinateur comme « cible » de l'infraction. C'est le cas de l'O.C.D.E. qui nous propose comme définition :

«L'entrée, l'altération, l'effacement et/ou la suppression de données et de programmes, dans l'intention de commettre un transfert illégal de fonds ; au fait de commettre un faux ou d'entraver le fonctionnement du système informatique et/ou de télécommunication. De même, la violation du droit exclusif du détenteur d'un programme informatique protégé, dans l'intention de l'exploiter commercialement et de le mettre sur le marché, ou l'accès dans un système informatique et/ou de télécommunication ou l'interception d'un tel système, fait sciemment et sans autorisation du responsable du système, en violant les règles de sécurité ou dans une intention malhonnête ou nuisible »[118].

Cette définition distingue l'accès dans un système informatique de l'exercice d'une influence sur les données qu'il contient. Elle intègre au même niveau dans la criminalité informatique, la contrefaçon et son exploitation commerciale dans un logique de marché. Elle met en évidence les éventuelles atteintes au droit de la concurrence dans ce domaine. Dans le même sens, ROSENBLATT a définit la criminalité informatique comme : « *Une activité illicite visant à altérer, modifier ou à effacer les informations inclus dans l'ordinateur* »[119]. Aussi, M. GRABOSKY considère que « *la criminalité informatique recouvre les illégalités impliquant des systèmes informatiques comme instruments ou cibles des infractions* »[120]. En Allemagne, 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. Il s'agit de « *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* »[121].

Cependant, nous pensons avec M. DELEPELEERE que voit que ces définitions sont trop vagues pour constituer des définitions « officielles » de référence[122]. En effet, si on se réfère, par exemple, à la définition adoptée en Allemagne, elle définit la criminalité informatique sur la base de faits qui ne sont pas avérés, sur lesquels porteraient simplement des soupçons. D'autres auteurs ont adopté des définitions exigeant la connaissance de la technologie de l'information. Selon M. D. TOMPSON « *la criminalité informatique est la criminalité commise par un auteur ayant une connaissance de la technologie de l'information* ».

[118] O.C.D.E : La Fraude Liée à l'Informatique : analyse des Politiques Juridiques (Paris), [1986] p. 72.
[119] M. ALEXANDER., *in* M. D. ROSTOCKER et R. H. RIENS: *Computer Jurisprudence Legal Responses to the Information Revolution* (N.Y., Ocena), [sans date] p. 104.
[120] P. GRABOSKY : *Computer Crime in a Borderless World* (Annales Internationale de Criminologie), [2000] Vol. XXXVIII n° 1/2 p. 67.
[121] W. SCHREIBER : La Délinquance Assistée par Ordinateur (R.I.P.C), [1997] 51 éme année, n° 464 p.9.
[122] *Précité.*

Enfin, des auteurs regroupent sous le vocable de criminalité informatique, plusieurs délits. C'est le cas du Conseil de l'Europe qui recense dans son *Rapport final d'activité sur la criminalité informatique en relation avec l'ordinateur* les délits que le droit européen doit réprimer. Il s'agit de : (a) la fraude, (b) le faux en informatique, (c) le sabotage, (d) la reproduction non autorisée d'un programme informatique protégé, (e) l'espionnage, (f) l'altération des données et des programmes informatiques , (g) les dommages affectant des données et des programmes [123]. De son coté, M. MANDELL distingue (a) l'usage d'un ordinateur pour commettre des actes illégaux lesquels fourniront des avantages financiers, et (b) les menaces visant l'ordinateur lui-même, c'est le cas du vol des matériels ou des logiciels, ou le sabotage et le piratage informatique[124].

Ainsi, il convient de s'affirmer que la cybercriminalité et la criminalité informatique ont deux domaines différents. La criminalité informatique représente « *toute action illicite perpétrée à l'aide d'opération électronique contre la sécurité d'un système informatique ou de données qu'il contient, quelque soit le but visé* »[125], alors que la cybercriminalité au sens strict du terme s'entend de l'ensemble des infractions commises à l'aide ou contre un système informatique connecté au réseau de télécommunication. La cybercriminalité quant à elle, a un domaine plus étendu puisque outre les atteintes contre les biens informatiques réalisables au moyen de l'Internent. Elle recouvre également nombre d'infractions contre les personnes et les biens qui peuvent être commises sur le réseau. Dans cette optique, la criminalité informatique et la cybercriminalité ont un domaine commun lorsque des infractions informatiques sont commises par l'usage du réseau de télécommunication. Mais toute infraction informatique n'est pas forcément commise au moyen d'un réseau de télécommunication. Et toute infraction commise au moyen d'un réseau de télécommunication n'est pas systématiquement une infraction informatique.

[123] Conseil de l'Europe : Rapport Final d'Activité Sur la Criminalité Informatique en Relation avec l'Ordinateur (Comité européen pour les problèmes criminels), [avril 1989] pp. 27-55.
[124] S.MANDELL: *Computer, Data Processing and Law* (St. Paul, Minnesota, West Publishing), [1984] p. 155.
[125] N. EL CHAER : La Criminalité Informatique devant la Justice Pénale (Thèse, Poitiers), [2003] p. 19 ; voir aussi P. AUVRET : La Détermination des Personnes Responsables (Paris, Gaz. Pal.), [mai 2002].

2. La cybercriminalité et la criminalité en col blanc

16. C'est l'auteur américain SUTHERLAND qui a le premier mit en évidence la délinquance en col blanc « *white collar crime* » dans son étude (*white collar criminality – 1939)* cherchant les raisons des différences de taux de criminalité suivant les nations. Selon lui, il s'agissait de criminalité des classes supérieures en lien avec leurs affaires, leur culture et leur milieu professionnel[126]. De son coté, H. EDELHERTZ a proposé une définition, acceptable en 1970, quand il décrit la criminalité en col blanc comme : « *Un acte illégal perpétré sans le recours à la contrainte physique usant de la dissimulation ou l'artifice, afin d'obtenir de l'argent ou des propriétés, éviter un paiement ou de perte de l'argent ou pour obtenir des affaires ou des avantages personnels* » [127] . Il ressort de cette définition qu'un système informatique est l'outil parfait pour une telle criminalité qui agit par « dissimulation », « sans contraintes physiques ». Cependant, il y a souvent une confusion entre la criminalité en col blanc et la cybercriminalité. Une des raisons est fournie par la fraude. Tandis que quelques auteurs classent la cybercriminalité sous la catégorie de la criminalité en col blanc (LEVI et COMER), d'autres comme PARKER, trouve que la cybercriminalité diffère de la criminalité en col blanc, comme cette dernière diffère de la criminalité de la rue[128].

MM. CLINARD et QUINNEY[129] voient que la criminalité en col blanc peut être considérée comme ayant lieu à trois niveaux. Le premier concerne *la criminalité d'entreprises*, où quelques infractions sont commises par des personnes officielles pour leurs sociétés. C'est le cas de l'espionnage industriel utilisant un système informatique ou la manipulation des fichiers informatiques, des comptes, des bilans, et des déclarations des impôts[130]. Le second niveau inclut les *infractions dévouées par des personnes utilisant leurs occupations et leurs métiers*. On peut citer par exemple le vol des matériels, des logiciels ou des fichiers informatiques. Enfin, le troisième niveau

---

[126] G. GEIS: *White-Collar Crime: Offences In Business, Politics And The professions* (N.Y, The Free Press), [1995] pp. 23-26. Si dans le langage savant on parle de « crime en col blanc » ; en langage courant on évoque une « magouille politico-financière ». Il s'agit d'infractions subtiles commises par des personnes que leur statut social éminent place a priori au dessus de tout soupçon. Elles devraient être réprimées avec la plus grande rigueur, dès lors qu'elles sont le fait de personnes ayant abusé de leur situation privilégiée.

[127] H. EDELHERTZ: *The Nature, Impact and Prosecution of White Collar Crime* (US Governement, Washington, DC), [1976] p.3.

[128] D.-B. PARKER: *Computer – Related White Collar Crime*, in Geis and Scotland, *précité.*

[129] M. CLINARD et R. QUINNEY : *Criminel Behaviour Systemes* : *A Typology* (N. Y, Rinehart & Winston), [1967] p. 131.

[130] Sur ce point M. ROSE déclare que beaucoup d'informaticiens considèrent comme normal d'employer illicitement des mots de passe, de copier des logiciels ou d'utiliser à des fins personnelles l'ordinateur de l'entreprise. Voir P. ROSE: La Criminalité Informatique (PUF, Coll. Que-sais-je ?) [1989] p. 54.

inclut les *infractions commises par des personnes hors de la société*. Il peut prendre la forme d'accès illégal à un système informatique, voyant des matériels confidentiels, commettant la fraude informatique, etc.

Les similitudes avec la cybercriminalité apparaissent ainsi très claires. Certains auteurs considérant même quelques délits informatiques comme une sous catégorie de la criminalité en col blanc[131]. Dans un premier temps, quelques types de ces deux infractions visant un avantage financier[132]. Ensuite, la cybercriminalité, n'exige pas le recours à la contrainte physique. Le cybercriminel se servant uniquement de son ordinateur pour commettre son infraction[133]. Enfin, les deux infractions exigent également que les malfaiteurs ne soient pas de « simples » criminels, ayant des connaissances spécifiques, comme la comptabilité ou encore, évidemment, la maîtrise des N.T.I.C[134].

Par contre, nous relevons avec M. DELEPELEERE un certain nombre de différences non négligeables entre la cybercriminalité et la criminalité en col blanc[135]. D'une part la criminalité en col blanc vise toujours des objets d'ordre économique, la cybercriminalité poursuit également d'autres buts, à caractère politique par exemple (comme le cyberterrorisme)[136]. D'autre part, si la criminalité en col blanc menace le monde de l'entreprise, la cybercriminalité menace également les particuliers, voir même les Etats. En conclusion, il convient d'affirmer que si la cybercriminalité présente des interactions avec la criminalité en col blanc, il n'en reste pas moins que certains délits informatiques ne rentrent pas dans cette catégorie. De même, la criminalité en col blanc est multiple et conditionnée par la nature de l'infraction commise[137] . Par conséquent, il serait insuffisant de s'arrêter à l'assimilation du fraudeur informatique au criminel en col blanc, pour chercher à en obtenir l'image réelle sans regarder les études criminologiques d'autres formes de déviance[138].

---

[131] P. GLINEUR: Droit et Ethique de l'Informatique (Bruxelles, Story Scientia), [1991] p. 180.
[132] P. DELEPELEERE, *op.cit.*
[133] *Ibid*
[134] *Ibid.*
[135] P. DELEPELEERE, *op.cit.*
[136] *Ibid.*
[137] H. CROALL: *Understanding White Collar Crime* (Buckingham, Open University Press), [2001] pp.1-6.
[138] Particulièrement ceux impliquant la destruction, le vandalisme, et les différents formes d'infractions qui impliquent la démonstration des compétences techniques des cybercriminels.

3. La cybercriminalité et la criminalité de haute technologie

17. La criminalité de haute technologie selon Monsieur D. MARTIN est la criminalité qui recouvre l'ensemble des actes illégaux intéressant l'informatique et les télécommunications tant sur le plan des matériels que des logiciels[139]. Elle concerne la criminalité informatique proprement dite et la contrefaçon / le clonage de composants électroniques capables de créer des dysfonctionnements dans les systèmes d'information, de télécommunications ou autorisant un usage frauduleux[140]. Dans cette optique, la criminalité de haute technologie peut couvrir deux catégories :

- Les infractions liées aux systèmes informatiques non connectés aux réseaux de télécommunication.
- Les infractions liées aux systèmes informatiques connectés aux réseaux de télécommunication.

Par rapport à notre définition de la cybercriminalité[141], le premier type d'infractions ne tombe pas sous cette catégorie. En revanche, la seconde catégorie d'infractions peut être classée sous la catégorie de la cybercriminalité, dans la mesure où les infractions impliquant, par un moyen ou par un autre un réseau de télécommunication. Dans cette optique, nous pouvons affirmer que quelques infractions de haute technologie peuvent être considérées comme des cybercriminalités et que d'autre, en revanche ne peuvent pas l'être.

B) – La distinction relative aux auteurs de l'infraction

18. Parce qu'elle est difficile à conceptualiser, la cybercriminalité est une source de confusion terminologique. Certains auteurs désignant les délinquants ou qualifiant les actes qu'ils réalisent, commettent quelquefois des confusions de sens en désignant, sous la terminologie de « *hacker* » ou « pirate » tous les délinquants en informatique[142]. Il convient donc de s'attarder sur les termes caractérisant ce délit, afin d'éviter les confusions terminologiques concernant le « *hacker* » (**1**), le cracker, et le crasher (**2**).

---

[139] D. MARTIN : Crime Informatique et Cyber-Guerre (Centre Universitaire Juridique de Recherche sur les Menaces Criminelles Contemporaines), [1999], disponible sur :
<http://strategique.free.fr/> (consulté le 17/05/2005).
[140] *Ibid*.
[141] Voir supra 13.
[142] D.- B. PARKER: *Fighting Computer Crime* (N.Y., Wiley),[1998], *op. cit*. p. 143.

1. Le Hacker

19. Dans l'esprit de beaucoup, les *hackers* sont tous ceux qui utilisent les N.T.I.C. à des fins contraires à la loi[143]. Ce n'est en réalité absolument pas la bonne définition. Le terme « *hacker* » ne se contente pas d'une définition unique. D'origine anglo-saxonne, il appartient désormais au langage courant. Le dictionnaire de la langue anglaise Collins Cobuild en propose dans son édition de 2000, deux définitions [144] :

> a**.** Un hacker informatique est quelqu'un qui tente de s'introduire dans les systèmes informatiques, en particulier pour obtenir des renseignements secrets ou confidentiels qui y sont entreposés.
>
> b**.** Un hacker informatique est quelqu'un qui utilise beaucoup l'ordinateur, notamment au point de n'avoir plus de temps pour quoi que ce soit d'autre.

Le terme *hacker* provient du verbe *hack* ; *to hack*, qui signifie la pénétration à l'intérieur d'un système informatique ou un ordinateur[145]. Le *hacker* peut être considéré comme« *une personne qui prend du plaisir à explorer en détail un système programmable et qui cherche sans cesse à étendre ses connaissances dans ce domaine*»[146]. Selon le *New Hacker's Dictionary*, le terme *hacking* signifie : (a) toute personne qui s'intéresse à explorer les systèmes informatiques ; (b) un expert dans une langue particulière (C+, C++) ou dans un domaine des système d'exploitation ; (c) une personne forte dans les détails de la programmation ; (d) une personne qui s'intéresse au défi intellectuel ; et (e) une personne qui essaie de découvrir les informations sensitives**[147]** .Il revêt deux actes : passer le temps devant un système informatique ; et entrer à l'intérieur de ce système. Ce sens semble être celui retenu à l'origine, dans les années 1960 au *Massachussetts Institute of Technology*[148], pour caractériser les *hackers*. A l'époque, ce terme désignait les programmeurs passionnés par leur travail [149]. Aussi,

---

[143] Disponible sur :
<http://espace-terre.info/blog?2006/02/27> (consulté le 03/06/2006).

[144] Traduit de l'anglais : hacker / hackers : 1. *A computer hacker is someone who tries to break into computer systems, especially in order to get secret or confidential information that is stored there.* 2. *A computer hacker is someone who uses a computer a lot, especially so much that they have no time to do anything else.* Disponible sur: <http://www.geocities.com/stefinem77/page1.html> (consulté le 04/06/2006).

[145] Dictionnaire Larousse : Français Anglais, édition 1999.

[146] D. Martin, et F.-P. MARTIN, *op.cit*. p. 75.

[147] D.-B. PARKER: *Fighting Computer Crime, op. cit.* p. 160.

[148] Le *Massachusetts Institute of Technology* est un des principaux centres universitaires ayant contribué à la recherche sur le réseau.

[149] J. CHIRILLO: *Hack Attacks Encyclopedia: A Complete History of Hacks, Cracks, Phreaks, and Spies over Time* (Canada, John Wiley), [2001] pp. 2-4.

le terme *hacking* est synonyme de *piracy*, donc de contrefaçon[150]. Conférant ainsi au terme « *pirate* » deux notions principales : la première désignerait la personne entrant par effraction à l'intérieur d'un système informatique [151] , et la seconde désignerait le contrefacteur, lorsqu'il est utilisé au sens de « *piracy* »[152]. Dans cette optique, le caractère polysémique du mot « piratage » semble se confirmer avec la définition du pirate que propose l'office québécois de la Langue Française (OLF)[153]. Ce dernier définit le pirate informatique comme « *le criminel informatique qui exploite les failles dans une procédure d'accès pour casser un système informatique, qui viole l'intégrité de ce système en dérobant, altérant ou détruisant de l'information, ou qui copie frauduleusement des logiciels* »[154].

Nous pouvons, selon cette définition distinguer trois formes de piratage informatique : (a) la pénétration des réseaux et systèmes informatiques ; (b) la copie frauduleuse des logiciels ; et (c) l'utilisations des programmes comme le cheval de Troie pour accéder aux systèmes informatiques. De son coté, le législateur français incrimine l'intrusion à l'intérieur d'un système de traitement automatisé de données sans se référer à la reproduction sans autorisation des programmes, laquelle relève du domaine des articles L. 335-2 et L. 335-3 du Code de la propriété intellectuelle. L'acte de contrefaçon n'étant pas rattaché au Code pénal, il ne saurait être rattaché à la fraude informatique, au sens de la loi du 5 janvier 1988. Ce constat conduit à distinguer le sens commun du piratage informatique, de sons sens juridique[155]. Le mot « *piratage* » ne figurant dans aucun texte de loi, la doctrine en a cependant précisé le sens juridique en le définissant comme « *le fait de dupliquer un programme, qui, à la différence du vol, est beaucoup plus subtil dans la mesure où il suppose une certaine habileté technique, et ouvre au pirate la maîtrise de la création logicielle d'un tiers sans que pour autant, ce tiers soit nécessairement dépossédé de sa création, même si le piratage peut indubitablement lui faire perdre une large part des bénéfices qui peuvent être attachés à l'exploitation de celle-ci* »[156].

En conclusion, il apparaît clairement que le piratage informatique s'entendrait juridiquement comme la reproduction sans droit d'un logiciel (au sens de *piracy*). Cela

[150] J.-F. CASILE, *op. cit.* p. 24.
[151] *Ibid*, voir aussi dictionnaire Collins Cobuild, *précité.*
[152] J.-F. CASILE, *op. cit.* p. 24.
[153] Office de la Langue Française (OLF), Gouvernement du Québec. Disponible à l'adresse : <http://www.olf.gouv.qc.ca/ > (19/11/2004).
[154] *Ibid.*
[155] J.-F. CASILE, *op. cit.* p. 24.
[156] *Ibid.*

permet d'attribuer à ce terme un sens juridique différent de son sens courant, ce qui échappe parfois à quelques professionnels du droit qui désignent à travers le pirate, autant le *hacker* que le *cracker*, ou le *phreaker*. Ces derniers, souvent confondus en pratique, se distinguent pourtant en raison de l'objet de leur acte.

2. Le Cracker, le Crasher, et le Phreaker

20. Le terme *crasher* provient du verbe *to crash* qui signifie « *s'écraser* »[157]. Il convient de proposer une définition de ce terme dans une logique comparative, en considérant le *crasher* comme la personne qui pénètre à l'intérieur d'un système informatique et détruit un de ses éléments par plaisir[158]. Dans cette optique, la distinction entre le *crasher* et le *cracker* est trouvée dans la finalité de l'infraction. Tandis que le *crasher* pénètre à l'intérieur d'un système informatique et détruit les données, le *cracker* soit détruit soit introduit des données dans ce système.

Le terme « *phreaking* » provient de la contraction des deux mots anglais *phone* (téléphone) et *freak* (monstre). On comprend par *phreaking* toutes les méthodes pour accéder illégalement à un système lié à la téléphonie[159]. Cela comprend la corruption et le détournement de PABX, de VMB, de téléphone portable, de modem...etc[160]. À cet égard, le *phreaker* désigne l'auteur d'une fraude informatique constituée par l'utilisation des lignes téléphoniques[161]. Beaucoup de vrais *hackers* ont été des phreakers afin de diminuer le montant de leur facteur téléphonique et pouvoir ainsi continuer leurs expérimentations et maintenir le contact avec les autres *hackers* [162]. L'émergence de l'Internet et la baisse des coûts de communication a partiellement réglé le problème. Les phreakers s'étant « reconvertis » dans le piratage des cabines téléphoniques ou des téléphones mobiles par exemple[163]. À titre de conclusion, il nous faut tout d'abord préciser que les termes les plus courants pour désigner les délinquants informatiques ne recouvrent pas toute la réalité de cette délinquance complexe. Les distinctions retenues entre le pirate, le *hacker*, le *crasher* et le *phreaker*, ne permettent pas de dresser une typologie des délinquants en informatique. Cependant, ces distinctions mettent en

[157] A. REY : LE Robert Micro : (Paris, Dictionnaires LE ROBER), [1998] p. 306.
[158] J.-F. CASILE, *op. cit.* p. 26.
[159] D. SHINDER, *op. cit*. p. 53.
[160] *Ibid.*
[161] W. SCHWARTAU: *Cybershock* (N.Y, Thunder's Mouth Press), [2000], p. 40.
[162] *Ibid*, p. 35.
[163] *Ibid*.

exergue une différence de nature, d'objet et de motivation, que le concept de cybercriminalité ne saurait à lui seul contenir.

CONCLUTION

21. Tout d'abord, une définition pratique de la cybercriminalité était nécessaire dès le début de cette recherche. D'elle-même, la définition est devenue une hypothèse de travail. La définition nécessairement large de la cybercriminalité que nous avons proposée est la suivante : toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite. Cette définition s'applique aux systèmes informatiques, au sens le plus large possible. Même si nous avons pu associer plus étroitement ordinateurs et fraude informatique, le problème de la spécificité serait resté entier. Ce problème a été en partie résolu, en affinant la définition de différentes manières.

Ensuite, nous avons vu que le phénomène de la cybercriminalité n'était pas une réalité spontanée, mais le fruit d'une longue évolution économique conduite par le développement accru des N.T.I.C. Cette nouvelle forme de criminalité connaît une ampleur exponentielle difficile à évaluer, laissant apparaître comme une évidence incontournable l'adaptation du système judiciaire[164]. La difficulté d'appréhender cette criminalité sur le réseau Internet tient en partie au fait que ce réseau est un moyen de communication mondial permettant de véhiculer tous types de données. L'appréhension des délits constatés sur ce réseau perd de sa netteté et se noie dans une approche globale de la criminalité, rendant de moins en moins visible une hiérarchisation de ces infractions, tant au niveau de leur nature juridique qu'au niveau de leur gravité. Une confusion gagne l'esprit du citoyen tendant à voir dans le réseau Internet la possibilité de commettre en toute impunité tous types de délits, allant de la criminalité artisanale à la criminalité organisée, sans entrevoir de frontières, de divergences de mobiles et de différences de profil d'auteur.

Enfin, face à ces atteintes, les législateurs avaient, dès le départ, des moyens différents d'agir dus soit à leurs règles pénales, soit à leurs traditions, et en conséquence,

[164] Voir aussi C. ATIAS et D. LINOTTE : Le Mythe de l'Adaptation du Droit au Fait (Paris, D.), [1977], Chron. p. 251.

des problèmes différents[165]. On peut, en schématisant quelque peu, avancer que trois types de techniques législatives ont été utilisés, tout en notant que ces différences d'attitudes tendent à s'estomper à l'heure actuelle : (a) certains Etats comme les Etats-Unis ont promulgué des législations spécifiques à la cybercriminalité qui couvrent ses différentes formes, en ne tenant pas compte des incriminations déjà existantes qui auraient pu s'appliquer à certaines types d'infractions ; (b) d'autres Etats ont procédé à l'analyse de leurs législations et de leurs lois pénales, ils les ont adaptées aux vus des nouvelles caractéristiques des méthodes de commission de l'infraction et ont établi de nouvelles incriminations pour couvrir ces infractions. Aussi, ils ont utilisé des législations spécifiques (droit d'auteur, loi sur la protection de la vie privée par exemple) pour réprimer quelques types d'infractions ; (c) enfin, il existe des Etats où les différentes formes de cybercriminalité pouvaient être couvertes par des dispositions législatives déjà en vigueur qui avaient une portée vaste, à savoir les dispositions sur l'accès non autorisé aux données et aux informations.

[165] En effet, l'adaptation du droit pénal au rythme des évolutions techniques « *qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient les services du cyberespace* » a motivé la création par le Comité européen pour les problèmes criminels d'un comité d'experts chargé de la cybercriminalité en novembre 1996 pour qui le droit pénal devait suivre le rythme des évolutions techniques et prévenir l'emploi à mauvais escient des services du cyberespace : « les rapides progrès des techniques de l'information ont des répercussions directes sur tous les secteurs de la société moderne. L'intégration des systèmes de télécommunication et d'information, en permettant le stockage et la transmission - quelle que soit la distance – de toute sorte de donnée, ouvre un immense champs de possibilités nouvelles. Ces progrès ont été favorisés par l'apparition des réseaux informatiques et des autoroutes de l'information, notamment l'internent ; grâce auquel toute personne ou presque peut avoir accès à la totalité des services d'information électronique, où qu'elle se trouve sur la planète. En se connectant au service de communication et d'information, les usagers créent une sorte d'espace commun, dit « cyberespace », qui sert à des fins légitimes, mais peut aussi donner lieu à des abus. Les infractions commises dans ce cyberespace le sont contre l'intégrité, la disponibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunication, à moins qu'elle ne consiste en l'utilisation de ces réseaux ou de leurs services dans le but de commettre des infractions classiques. Le caractère international des infractions en question- par exemple celles commises au moyen de l'Internet- se heurte à la territorialité des institutions nationales de répression. Le droit pénal doit donc suivre le rythme de ces évolutions techniques qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient, les services du cyberespace et de porter ainsi atteinte à des intérêts légitimes ». Voir Comité européen pour les problèmes criminels [103/21196].