LA CRIMINALITE INFORMATIQUE SUR L'INTERNET

Dr. Mohammed BUZUBAR
Dept. du drait Penal
Faculte de droit - Université du Koweit

Resumé:

L'internet est le miroir de la civilisation occidentale. Passé en quinze ans du stade restreint de mode de communication inter universitaire à celui de réseau planétaire, il épouse aujourd'hui les aspirations les plus louables comme les plus viles bassesses de nos contemporains. Les vices les plus répandus ont ainsi trouvé une place à leur aise dans un espace virtuel où se dévoloppe une criminalité bien réelle. Cette criminalité «assistée par ordinateur» est polymorphe et se retrouve dans tous les domaines de la vie économique et sociale concernés par l'avènement de l'Internet.

La criminalité informatique est spécifique du fait des techniques employées et de la personnalité de ses auteurs. Les implications sont multiples et les conséquences économiques lourdes pour les entreprises. Les milliards de pertes ainsi occaisionnés présent sur leur compélitivité. La dégradation de leur image de marque et de leurs parts de marché coexistent avec la nécessité d'investir en moyens de prévention et de protection. Le problème est similaire dans l'ensemble des pays développés, où le coût économique de la criminalité informatique augmente fortement et de façon régulière depuis une quinzaine d'années.

INTRODUCTION

Encore inconnu il y a quelques années ou réservé aux spécialistes de l'informatique, Internet ou l'Internet selon certains puristes, commence désormais à se développer auprès du grand public.

Selon la formule de l'ex-vice-Président américain Al Gore les autoroutes de l'information permettront la circulation du multimédia qui peut être défini comme "*un ensemble de services interactifs utilisant le seul support numérique, pour le traitement et la transmission de l'information sous toutes ses formes: textes, données, sons, images fixes, images animées réelles ou*

virtuelles"[1]. Selon Olivier Quéau, directeur de la division informatique et information de l'UNESCO[2]: "*Ce qui en train d'arriver est quelque chose de la même nature que ce qui est arrivé à l'Europe du 15ème siècle avec simultanément l'invention de l'imprimerie, la découverte de l'Amérique, l'apparition d'un phénomène comme celui de la Réforme; cette révolution du 15ème siècle, nous sommes en train de la vivre dans l'ensemble des pays développés. Cette révolution est une révolution de la représentation, de l'écriture, de l'imprimerie, d'un nouvel alphabet - l'alphabet, c'est le numérique -,l'imprimerie c'est Internet, la nouvelle Amérique, c'est le cyberespace*."

Effectivement, ces autoroutes de l'information et le multimédia modifieront radicalement notre mode de vie puisque dans cette nouvelle société, quasiment toutes les activités humaines transiteront par les réseaux[3]. Les réseaux ne permettront plus seulement aux universitaires de s'échanger le fruit de leurs recherches mais permettront également, comme ils commencent à le faire, de profiter de nouveaux espaces de jeux et de loisirs: nous pourrons écouter de la musique, regarder un film, visiter un musée virtuel. Les activités économiques et administratives ne seront pas en reste: déjà le commerce virtuel se développe, les administrations nous permettent progressivement de remplir nos formalités administratives à domicile et le télé-travail est amené à devenir la nouvelle forme d'exercice de sa profession. C'est ainsi qu'aujourd'hui, beaucoup de gouvernements, tendent vers l'informatisation des procédures administratives tel que le cas de l'Etat du Koweït.

L'on se doit de maîtriser les techniques indispensables à l'utilisation et la création de ces réseaux: dans notre intérêt individuel si l'on ne veut pas faire partie des exclus de cette société.

Conscients de l'enjeu économique et culturel que peut représenter cette nouvelle forme de communication, il y a en France un million d'utilisateurs dont entre 250 000 et 300 000 abonnés individuels[4], mais les Etats-Unis en comptent plus de 40 millions (soit dix fois plus, rapporté au nombre

(1) G. THERY, Rapport Officiel *Les autoroutes de l'information*, La Documentation Française, p.14, 1994.

(2) émission: " Allô la terre - les autoroutes de l'information " - La Cinquième - du 17 au 20 nov. 1997

(3) G. THERY, le Rapport Officiel *Les autoroutes de l'information*, (p.61 &s.) contient de nombreux exemples

(4) Selon une étude de l'Aftel (Association française de télématique) - Le Monde 9 janvier 1998.

d'habitants), dont 47%. de femmes[5]. Au Koweït, le nombre des utilisateurs d'un tel service, s'élève à 150000 abonnés individuels[6].

En effet, comme a pu l'expliquer Joël de Rosnay, le directeur de la stratégie à la Cité des Sciences et de l'Industrie[7], les autoroutes de l'information comme Internet ne sont pas des moyens traditionnels de communication devant lequel le spectateur est passif. Ces nouveaux moyens sont "interactifs", chacun intervient en tant que maille d'un réseau au sein duquel chacun est "consom-acteurs et non plus consommateur d'information".

L'Internet est le miroir de la civilisation occidentale. Passé en quinze ans du stade restreint de mode de communication inter universitaire à celui de réseau planétaire, il épouse aujourd'hui les aspirations les plus louables comme les plus viles bassesses de nos contemporains[8]. Les vices les plus répandus ont ainsi trouvé une place à leur aise dans un espace virtuel où se développe une criminalité bien réelle. Cette criminalité "assistée par ordinateur" est polymorphe et se retrouve dans tous les domaines de la vie économique et sociale concernés par l'avènement de l'Internet[9].

Pour comprendre la criminalité informatique qui peut y être associée, il faut alors étudier plus précisément son histoire (I), ce qui nécessite, pour une meilleure appréhension de connaître son fonctionnement (II), et les services accessibles (III).

(I) HISTORIQUE

Au début des années soixante, deux informaticiens, Robert Taylor et Joseph C.R.Licklider se rendirent compte que les énormes ordinateurs de l'époque qui fonctionnaient de façon isolée et selon des langages différents devaient pour devenir plus efficaces, communiquer ensemble. Cette idée fut exploitée par l'A.R.P.A (Advanced Research Pojects

(5) Selon une étude des instituts Intelli-Quest Information Group et Zona Research - Le Monde 20 décembre 1997

(6) Selon la statistique de Qualitynet.

(7) émission: " Allô la terre - les autoroutes de l'information " - La Cinquième - du 17 au 20 nov. 1997

(8) F-J.PANSIER, La criminalité sur L'Internet, Puf, 2000, p.3.

(9) "*Le premier délit informatique identifé est commis aux Etats-Unis en 1966, il s'agissait d'une altération des comptes d'une banque de Minneapolis*"; Frédéric-Jérome.P, La criminalité sur l'Internet, Que sais-je?, Puf, 2000, P.95.

Agency - l'agence de recherche du Ministère américain de la Défense) qui mit au point le premier réseau: l'A.R.P.A net (c'est à dire le " réseau de l'A.R.P.A ").

Le but était de relier différents ordinateurs pour qu'ils puissent s'échanger des données. Il fallut donc mettre au point un protocole informatique, c'est à dire un ensemble de règles permettant aux machines de dialoguer, et ce fut N.C.P (Network Control Program).En ce qui concerne la fiabilité des connexions, l'objectif était de protéger le dialogue de toute interruption. Ces recherches s'étant effectuées durant la Guerre Froide, la " légende " veut que l'armée américaine travaillât surtout à empêcher une défaillance due à l'explosion au-dessus du territoires des Etats-Unis d'une bombe nucléaire soviétique(10). Plus prosaïquement, les chercheurs tentaient de surmonter les conséquences de la simple rupture d'un lien de connexion. L'idée fut donc de communiquer en réseau: Il n'y a pas d'ordinateur central, ce qui évite toute paralysie du système en cas de simple défaillance à ce niveau et au lieu de prévoir un lien entre chaque ordinateur, ce qui nécessite des travaux considérables et on l'a vu, est peu prudent, chaque ordinateur sera relié aux ordinateurs les plus proches et ainsi de suite La comparaison la plus parlante est celle de la toile d'araignée: De la même manière que l'araignée qui veut se déplacer sur sa toile, le message émis par un ordinateur A à un ordinateur Z relira ces deux points en empruntant le lien qui peut unir l'ordinateur A à l'ordinateur B, puis celui entre l'ordinateur B et l'ordinateur C et ainsi de suite jusqu'à ce que le message parvienne à l'ordinateur Z. Chacun des ordinateurs-relais est un nœud (node) par lequel le message transite. Si une ligne est interrompue ou surchargée, le message passe par une autre ligne. Nous verrons ultérieurement plus précisément ce fonctionnement.

La première connexion empruntant ce réseau relia le 21 novembre 1969 l'université de Santa Barbara (Californie) à celle de Stanford (Utah) en utilisant comme noeud un ordinateur de l'université de Los Angeles.

(10) Hounicoute.J., Internet, éd academia international, 1997, p.18; B.Norton & C.smith, *Understanding business on the internet in week*, éd Hodder&Stoughton,1997, pp.9-12.

Dès lors, l'existence de l'Internet ne tenait plus qu'à la participation au réseau du plus de nœuds possibles.

Pour cela, l'Américain Vinton Cerf invente en 1974 un langage commun: le TCP/IP (Transmission Control Protocol / Internet Protocol).

Au début des années quatre-vingt, se créèrent des stations de travail qui fonctionnaient sur la norme Ethernet c'est à dire une norme de réseaux reliant des machines dans un rayon de plusieurs centaines de mètres. Puis ces réseaux locaux sont connectés entre eux grâce à l'unité de langage employé. En 1983, le Ministère de la Défense américain scinda ARPAnet en deux réseaux, l'un civil (ARPAnet) et l'autre militaire (Milnet). En 1985, le NSF (National Sciences Foundation - une agence gouvernementale américaine finan5ant la recherche) créa ce qui fut sans doute le plus grand réseau de l'époque: le NSFNET qui intégra ARPAnet.

D'autres réseaux, accessibles les uns aux autres existaient aussi: Ainsi, USENET fut créé par la communauté scientifique pour débattre de questions variées au sein de (News Groups).

Comme nous l'avons vu, les réseaux étaient essentiellement réservés à la recherche militaire et universitaire. Mais en 1989, cette nouvelle forme de communication devint accessible à tout à chacun (à la condition de posséder un ordinateur équipé). A partir des travaux de Timothy Berners-Lee , le CERN de Genève (Centre Européen de Recherche Nucléaire) mis au point le concept du World Wide Web qu'on appelle également le WWW ou W3. Son nom exprime tout à fait la nature des réseaux puisque que sa traduction signifie "toile d'araignée mondiale". Ce réseau permet à son utilisateur de découvrir de nouvelles informations en cliquant simplement sur un mot. A partir de 1993, l'utilisation en devient encore plus simple grâce à la création de Mosaic, puis de Nestcape, des logiciels qui permettent à tout profane de naviguer simplement sur la toile (ce sont des browsers ou "butineurs", "navigateurs")

(II) LE FONCTIONNEMENT

Expliquer comment les informations voyagent d'un ordinateur à un autre, même si cela est fait de façon schématique, est nécessaire pour

mieux appréhender la délinquance qui peut sévir sur le réseau ainsi que les difficultés de poursuites que l'on rencontrera.

Les réseaux sont seulement des réseaux - contenu (l'information) mais aussi des réseaux physiques. Les différents ordinateurs doivent être reliés matériellement les uns aux autres pour pouvoir s'échanger des informations. Ces liens peuvent être de quatre ordres : soit des cãbles téléphoniques, soit des cãbles coactiaux, soit des fibres optiques, soit des émetteurs - récepteur (réseaux satellites ou hertziens). L'information (le son, les images, les textes) est convertie en données numériques et y circule sous forme d'ondes ou d'impulsion électriques.De plus, il faut indiquer que ce sont des réseaux à commutation de paquets (l'envoi est mêlé à d'autres et ne s'attribue pas un tronçon du réseau comme peut le faire un réseau à commutation de circuit).

Les multiples connexions de certains ordinateurs entre eux vont ainsi permettre de communiquer d'un ordinateur à un autre distant. L'utilisateur s'adressera, grâce au modem dont est doté son ordinateur, à un fournisseur d'accès (on parle aussi de fournisseur de services ou de *provider*) connecté au réseau. Ce dernier est soit un opérateur directement relié à Internet aux Etats-Unis (il en existe deux au Koweït : Kemes, Qualitynet), soit un fournisseur d'accès qui loue à l'un des opérateurs cités de la bande passante pour la sous-louer. Le fournisseur d'accès relèvera l'adresse du destinataire et "traduira" le message selon le protocole IP. Le message voyagera en paquets. Chacun d'entre eux contiendra l'adresse du destinataire, une partie du message et sa place dans le message. Ainsi, chaque paquet pourra emprunter des chemins différents pour arriver à destination, les itinéraires étant différents selon l'encombrement ou la rupture des liens. Tous les paquets seront acheminés chez le fournisseur d'accès du destinataire, qui reconstituera le message. Dès lors, il le laissera à la disposition du destinataire.

Cette technique permet d'offrir aux utilisateurs différents services et permet à différents acteurs d'intervenir.

(III) LES SERVICES ACCESSIBLES

Quatre types de services s'offrent à l'utilisateur d'Internet aujourd'hui.

*** La messagerie électronique**

Ce service, qui est le plus utilisé sur Internet (2 700 milliards courriers échangés en 1997[(11)]), permet à chacun d'envoyer ou de recevoir des messages ou des fichiers informatiques. De la même manière que le courrier postal, ce courrier électronique (ou E-mail) nécessite du destinataire une adresse électronique. Le courrier sera rapatrié chez le fournisseur d'accès du destinataire sur lequel se situe la boîte à lettres électronique (BAL) du destinataire qui la consultera quand il voudra.

Les avantages de cette correspondance sont nombreux par rapport à la correspondance traditionnelle :

- la rapidité de réception: les communications ne prennent qu'une à deux minutes pour traverser l'Atlantique et fonctionnent 24 heures sur 24;
- le faible coût: même si le destinataire se situe à des milliers de kilomètres, l'expéditeur ne paye que la communication entre son domicile et son fournisseur d'accès;
- la nature des messages: par ces messageries, l'on peut envoyer aussi bien du texte que du sons, ou des images;
- la facilité de lecture du message: le destinataire peut utiliser n'importe quel ordinateur pour ouvrir sa boîte à lettre;
- l'utilisation du message: le message peut être lu sur l'écran, conservé, imprimé, envoyé à une autre personne.

Le courrier électronique peut ne pas être réservé à un seul destinataire. C'est sur ce principe que fonctionnent les *mailing lists*. En s'inscrivant sur une de ses listes de diffusion, on reçoit gratuitement par le biais de sa messagerie électronique les nouvelles livraisons d'un bulletin périodique.

(11) Selon une estimation du département du commerce américain, Le Monde 9 oct. 1997

*** Les forums de discussions**

Ces forums ou *NewsGroups* sont des espaces de discussion thématiques situés sur le réseau *Usenet*. Il en existe plusieurs milliers (actuellement, on parle de 38 000 forums[12], dont les thèmes sont aussi divers que nombreux. Pour y accéder, il faut contacter le serveur qui gère ce forum. On peut alors y consulter les derniers échanges, poser des questions (avant il vaut mieux avoir consulter la FAQ: Foire aux questions) ou y laisser sa propre contribution.

Dans le même esprit, se développe l'IRC *(Internet Relay Chat)*, qui permet de dialoguer, toujours par écrit, en direct avec les autres personnes connectées. Il existe même des IRC en trois dimensions où chacun se représente sous la forme d'un avatar qui peut se déplacer dans un décor virtuel.

*** Le transfert de fichiers**

Les applications Telnet et FTP permettent de se connecter à distance et de récupérer des données par téléchargement.

FTP *(File Transfer Protocol)* permet de rapatrier sur son ordinateur des données pour une utilisation ultérieure. Le plus souvent, cela servira à transférer des logiciels soit gratuits *(freewares)*, soit soumis à une obligation morale de rémunération *(sharewares)*. Dans le sens inverse, il permet également d'envoyer des fichiers de son ordinateur à une autre machine. En principe, pour ces opérations, il faut obtenir l'accord du réseau interlocuteur : télécharger des données auxquelles l'ont n'a pas droit ou ajouter des données non désirées par le destinataire est évidemment condamnable. Dans l'autre sens, celui qui télécharge des informations peut attraper de cette manière un virus.

Telnet ne permet pas par contre de télécharger des fichiers. C'est un système qui permet uniquement de se connecter à distance sur un ordinateur afin de le piloter. Si l'utilisation de cette application nécessite d'avoir les autorisations pour accéder aux systèmes, généralement d'entreprises ou de centres de recherche, elle est sans doute accessible à

(12) "Internet, la toile d'araignée informatique " Armées d'aujourd'hui, n°227 février 1998, p.65

un pirate informatique qui désirerait modifier des données de l'ordinateur destinataire.

*** Le World Wide Web**

Le *Web* (ou encore W3, WWW ou " la toile ") est sans aucun doute le service le plus connu du grand public. Crée en 1989, c'est un système de présentation et de consultation des informations multimédia. Pour accéder à un site, il faut le joindre grâce à son adresse : son URL *(Uniform Resource Locator)*. Celle-ci peut être fournie à l'utilisateur par un moteur de recherche (comme Yahoo, AltaVista...) L'on peut de plus, et c'est l'originalité du *Web*, " surfer " grâce au système de navigation "hypertexte": en cliquant sur des mots-clés ou des icônes, l'on découvrira de nouvelles pages ou de nouveaux sites.

De la même manière que les forums, les sites élaborés par les éditeurs de contenu et hébergés par des serveurs d'hébergement (qui peuvent être également éditeurs ou fournisseurs d'accès) sont excessivement nombreux et d'une diversité sans fin. C'est pourquoi certaines difficultés peuvent se poser: le contenu peut être considéré comme répréhensible, les informations fournies ne sont pas forcément exactes et difficilement vérifiables. Ces informations seront de plus, comme toute page d'un ordinateur enregistrables et imprimables.

S'il est clair pour tous que la criminalité dans le cyberespace nécessité la mise en œuvre urgente de moyens importants, les instruments actuels de répression doivent être améliorés pour une meilleure efficacité.Seulement, le conflit actuel entre autorégulation (régulation par les acteurs de l'Internet: professionnels et utilisateurs) et régulation de type Etatique (processus vertical de contrôle) paralyse toute concertation internationale et toute prise en compte globale du phénomène. Le préjudice est d'autant plus grave et la carence d'autant plus malheureuse qu'il s'agit en fait d'un faux débat, la meilleure façon de limiter la cybercriminalité étant de concilier les deux. Si la mise en place d'une organisation internationale aux pouvoirs répressifs délégués par les Etats membres et acceptés pas les utilisateurs de l'Internet doit encore être taxée d'utopique, on désigne par le terme corégulation toutes les autres

solutions plus consensuelles de conciliation. Il s'agit d'une norme législative ou non, née d'une concertation entre les pouvoirs publics et les partenaires sociaux oeuvrant dans les nouvelles technologies.

L'appréhension uniforme d'Internet est encore compliquée par son caractère hybride, à la fois système informatique et support de nombreux médias. Les grands axes de cyber-criminalité ne répondent pas, loin de là, aux mêmes motivations ni aux mêmes moyens, et peut-être faudrait-il différencier les moyens mis en œuvre pour lutter contre ces divers fléaux **(Partie 1: l'information objet d'infraction)**. A cet effet, il est nécessaire de rechercher des moyens de lutte adaptés à la structure quasi insaisissable d'Internet **(Partie 2: l'encadrement juridique de la cyber-criminalité)**. Ils peuvent prendre la forme d'une coopération entre l'Etat et les organismes professionnels, quitte même à forcer certaines normes communes ou encore à instaurer un droit applicable à l'Internet, voire un droit de l'Internet, par adaptation des règles existantes, par exemple par l'instauration systématique de délits obstacles pour contrer les difficultés de preuve inhérentes au réseau des réseaux.

Dans ce cadre, nous nous intéresserons spécialement à la législation pénale, actuellement en vigueur au Koweït, pour voir à quel point elle pourrait faire face à ce type de criminalité. Soulignons ici que jusqu'à ce jour, il n'existe pas de législation spécifique contre la criminalité informatique, ce qui résulte un vide juridique que nous souhaitons voir rapidement combler. Il est à noter dans ce domaine que le Koweït est l'un des pays de la région les plus avancés dans l'usage du réseau Internet. Ainsi est-il très important d'évoquer le rôle du Droit comparé, auquel nous aurons souvent recours, dans le cadre d'une comparaison étroite avec le droit Français.

PARTI 1: L'INFORMATION OBJET D'INFRACTION

Personne ne peut aujourd'hui sous-estimer l'information et les avantages de l'usage de l'informatique qui a su conquérir tous les domaines de la vie quotidienne, tel que l'a exprimé M. Bart de SCHUTTER: "*L'informatique a laissé d'importantes traces dans notre vie de tous les jours, et c'est grâce à elle que revient le développement et l'amélioration de beaucoup d'activités tant de part leurs formes que leurs contenus*"(13). Cependant cet usage intensif n'a pas que des aspects positifs étant donné qu' il est fréquent de rencontrer des cas d'utilisation abusive et malintentionnée de l'informatique et qui se résume en la criminalité informatique. Cette nouvelle réalité sociale préoccupe beaucoup des jurisconsultes.

C'est la nouveauté et la pluralité des services sur ce nouveau mode de communication qui ont fait croire à l'émergence d'une zone de non-droit et à l'impossibilité de sanctionner les comportements répréhensibles sur Internet. La vérité est toute autre: comme le mentionne le rapport rendu par la Mission interministérielle présidée par Mme FALQUE-PIERROTIN(14) il n'y a pas "*vide juridique mais plutôt pléthore de textes de droit commun applicables à l'Internet*". Les incriminations ne manquent donc pas et peuvent couvrir la quasi-totalité des comportements condamnables **(Chapitre I)**. Les difficultés que rencontre la répression se situent plus au niveau de la pratique des poursuites qui se heurte à des délinquants dont le champ d'action est un réseau international, illimité et instantané, les cyber- criminels **(Chapitre II)**

(13) Bart de SCHUTTER, *Apropos de la fraud informatique*, Rev.Dr.Pen.crim, 1985, p.383.

(14) Rapport au ministre délégué à la Poste,aux Télécommunications et à l'Espace et au ministre de la *Culture Internet - Enjeux juridiques* - La Documentation Française coll.des rapports officiels

CHAPITRE I
LES COMPORTEMENTS CYBER-CRIMINELS

Esprits libertaires ou par exemple extrémistes politiques, les délinquants du cyberespace n'ont à priori que peu de ressemblances, et il semble difficile de leur appliquer un profil commun. Cela tient sans doute aux difficultés de définition de l'Internet même, tour à tour et parfois simultanément média, support, ensemble de services, et, même réalité nouvelle sous la plume de certains auteurs. Pourtant, toutes les infractions ne peuvent être transposées dans l'univers numérique. Citons, pour autant que cela puisse être nécessaire, le crime d'empoisonnement. D'autres, la plupart, peuvent en théorie être commises par le biais d'Internet. Mais alors de toute façon, le réseau des réseaux n'est qu'un accessoire fortuit de l'infraction.

Les comportements répréhensibles qui s'expriment sur et par Internet, ont pour point commun d'avoir trait à la fonction première du Net: la communication. Or la communication est interactive: on peut donc, soit se procurer des informations, soit en émettre.

De ce fait, on peut distinguer deux grands types de comportements répréhensibles: ceux qui ont pour support une information que l'auteur émet, qu'elle soit publique ou privée et ceux qui ont pour objet une information que l'on peut "recevoir".

Il est essentiel de souligner que l'Internet ne doit pas pour autant être " diabolisé ". Nous verrons dans les sections suivantes que la liste des infractions pouvant être commises via Internet est longue. Cependant, ce n'est pas Internet qui est criminogène, mais l'utilisation qui en est faite, comme cela est vrai pour tout instrument que le progrès nous apporte.

Au Koweït, la criminalité informatique ne soulève pas de problèmes particuliers étant donné que dans les textes pénaux actuellement en vigueur, le législateur incrimine déjà l'acte indépendamment du moyen utilisé mais peut y prévoire même des peines alourdies dans certains cas de figures.

Comme nous l'avons laissé entendre, le droit français est à même de réprimer ces comportements[15]. C'est ce que nous tenterons de démontrer en les étudiant suivant la distinction établie précédemment. Effectivement Il semble préférable d'étudier ces deux catégories de façon distincte dans la mesure où l'attitude du délinquant n'est pas la même; de ce fait, les incriminations en jeu sont différentes: la première hypothèse, est La Fraude Informatique (Section I.) tandis que la seconde est l'atteinte aux droits (Section II), et l'atteinte à la société (Section.III).

SECTION I: LA FRAUDE INFORMATIQUE

Nous l'avons déjà dit, tout message peut transiter par Internet et par là même, tout message porteur d'infraction. Les comportements condamnables susceptibles de se manifester sur le Net n'ont comme limite que l'imagination des internautes. Mais ces comportements sont identiques à ceux qui peuvent se manifester par les autres moyens de communication. Or le droit pénal français[16] a déjà pris des dispositions à l'égard de ces derniers, dispositions qui sont dès lors, susceptibles de s'appliquer à Internet.

Dans certaines hypothèses, l'information va concourir à un comportement délictueux. Ce peut être notamment le cas dans l'escroquerie **(A)**, et la vente de produits interdits **(B)**.

A) L'escroquerie

C'est le cas lorsqu'un internaute se sert d'Internet pour émettre à destination d'autres utilisateurs une information destinée à les induire en erreur afin de les déterminer à effectuer une remise. Un tel comportement a récemment été découvert par la Commission fédérale américaine du Commerce[17]. Une société new-yorkaise avait créé deux sites d'images

(15) Les règles générales en droit Koweïtien sont suffisantes pour la qualification et la répression de certains comportements, étant donné que le droit Koweïtien s'intéresse plus au résultat du crime qu'à l'instrument utilisé pour son exécution.

(16) La loi du 5 janvier 1988- dite loi Godfrain du nom de son initiateur- a mis en place des dispositions propres à la fraude informatique qui ont été intégrées dans le nouveau code pénal, entré en vigueur le 1er mars 1994, Art. 323-1à 323-7.

(17) Le Monde 8 nov. 1997, Bulletin de la criminalité informatique (Canada) avril 1997 http:// **www.rcmp-grc.ca/html**

pornographiques qui n'étaient consultables qu'après avoir téléchargé un logiciel graphique spécifique. Or ce logiciel permettait en réalité de déconnecter le modem de l'utilisateur de son fournisseur d'accès et de le reconnecter sur un serveur basé en Moldavie qui re-routait ensuite la requête au Canada. De plus, ces re-connexions demeuraient actives même lorsque l'ordinateur avait changé de site. Ainsi, les utilisateurs du site pornographique devaient payer non pas la communication locale avec leur fournisseur d'accès, mais une communication internationale, dont une partie des bénéfices profitait à la société éditrice.

A n'en pas douter, de tels faits tomberaient sous le coup de l'art. 313-1 C.P.F qui sanctionne l'escroquerie, c'est à dire le fait "*soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge*".

Le Code pénal Koweïtien quant à lui dans l'article 231 définit d'escroquerie comme étant: "*tout acte par lequel l'auteur a l'intention de tromper autrui ou l'induire en erreur, ou en extraire une somme d'argent, que ce soit fait oralement ou par écrit ce qui est le cas de l'acte d'escroquerie sur Internet*"[(18)].

Les escroqueries sur Internet peuvent prendre diverses formes. Par exemple celle d'une loterie: deux sociétés japonaises avaient organisé une fausse loterie qui avait attiré une centaine de joueurs ayant misé près de 900 000 F. Après avoir affiché les numéros prétendument gagnants, le site disparût[(19)].

B) La vente de produits interdits

Internet peut également être le support de la vente de produits contrefaits, quelque en soit la nature. Le réseau étant utilisé majoritairement par des gens qui s'intéresse à l'informatique, la vente de logiciels

(18) Art.231 du C.P.K.

(19) Selon le quotidien Asahi Shimbun, Le Monde 17 janvier. 1998

contrefaits est l'une des plus présentes (mais la vente de disques, cassettes et autres produits existe aussi).

Ce type d'entreprise de contrefaçon diffère de la contrefaçon "classique"[20] qui est présentée comme l'activité de spécialistes "*parfaitement informés et organisés, opérant avec de gros moyens financiers*", de "*véritables " industrie multinationales*". Internet permet aussi bien à ce type de grande entreprise qu'à tout particulier de se livrer à la contrefaçon et à la vente de ces produits, dans la mesure où la copie de logiciels est chose facile (copier un logiciel sur une disquette est un jeu d'enfant et les graveurs de CD-Rom sont désormais abordables) et que le Net facilite les prises de contact avec les acheteurs potentiels (le contrefacteur n'a pas besoin d'imaginer et de mettre sur pied un réseau de vente). C'est ce qui avait permis à deux jeunes français de la région de La Lorraine de vendre des contrefaçons des logiciels de jeux: ils avaient déplombé et dupliqué ces logiciels et les avaient vendus via Internet après en avoir fait la publicité dans un journal diffusé sur le réseau[21].

Or, la contrefaçon de logiciel est très préoccupante[22]. On estime qu'en France, 57% des logiciels utilisés sont des copies piratées et dans certains pays d'Asie du Sud-Est ou d'Europe Centrale le chiffre serait de 99%[23]. Cela représentait en 1994 une perte mondiale pour les développeurs et les éditeurs de logiciels de 76 milliards de francs (dont 3, 9 milliards au détriment de la France). Ce coût de la contrefaçon a évidemment des répercussions importantes: il entraîne une hausse des tarifs au détriment des acheteurs, un retard dans le financement et donc le développement de nouveaux produits, et pénalise l'emploi[24]. Toutes ces constatations sont relatives à l'ensemble des formes de piratage de

(20) P. BRUNOT COLL, *La contrefaçon*, Que sais-je, éd.PUF 1986.

(21) panorama de presse du SEFTI - 1er trimestre 1996

(22) J.P. COURTOIS, "*Combattre le piratage de logiciels*", Gaz. Pal. 12, 13 juin 1996 p.36

(23) En 1993, un audit portant sur 1022 machines du Pentagone a démontré que 51 % de ses ordinateurs étaient équipés de copies illicites; Expertises n°209 nov. 1997 p.329

(24) On considère, pour la France, que si le taux de piratage passait de 57 % à 35 %, l'industrie du logiciel pourrait employer 13 000 personnes supplémentaires.

logiciels, et on peut penser qu'Internet et sa facilité d'utilisation ne feront qu'accroître ce phénomène.

Au Koweït, il était très facile de se procurer des produits informatiques piratés, mis en vite publiquement et ouvertement même dans les rayons des magasins spécialisés. Cependant, sous la pression de la communauté internationale, oeuvrant pour la protection des droits d'auteurs l'état s'est vu dans l'obligation de décréter la loi 64/1999 (code de la propriété intellectuelle) incluant 49 articles. Cette loi s'est voulue conforme aux jurisprudences modernes, législations et conventions internationales.

C'est pourquoi le logiciel est protégé(25) au même titre que les autres œuvres de l'esprit énumérées par l'art. L.112-2 Code de la Propriété Intellectuelle Française. Si l'utilisateur du logiciel bénéficie d'un droit d'analyse (c'est-à-dire d'"*observer, étudier ou tester le fonctionnement du logiciel*") et d'un droit de compilation (qui consiste dans le droit d'établir "*la reproduction du code du logiciel ou la traduction de la forme de ce code*" art. L.122-6-1 IV C.P.I.F) par contre, l'art. L.335-3 C.P.I.F énonce que "*toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi*" constitue une contrefaçon, délit sanctionné(26) à l'encontre d'une personne physique d'une peine d'emprisonnement de 2 ans et d'une amende de 1 000 000 F (art. 335-2 C.P.I.F) et à l'encontre d'une personne morale d'une amende de 5 000 000 F (et de peines complémentaires dont la dissolution). Il faut remarquer que cette incrimination vise la reproduction, la représentation ou la diffusion du produit et non pas sa mise en circulation à des fins commerciales. L'art. 7 de la directive du Conseil des Communautés européennes du 14 mai 1991, relative à la protection juridique des programmes d'ordinateurs, visait ce type de comportement, mais cette disposition ne fut pas transposée. Il est vrai que les vendeurs peuvent être poursuivis du chef de la reproduction lorsqu'ils ont fait eux-mêmes les copies ou en tant que complices.

(25) Mémento guide BENSOUSSAN, *Le logiciel et le droit*, Dir. J.F. Forgeron, éd Hermès 1994
(26) Depuis la loi n° 94-102 du 5 février 1994

La France n'est pas le seul pays à s'inquiéter de la multiplication des contrefaçons de logiciels: Les Etats-Unis se sont dotés du *No Electronic Thief Act* qui punit de 5 ans d'emprisonnement et de 250 000 $ toute forme de copie illicite de logiciels, même occasionnelle ou sans but lucratif, dès lors que le manque à gagner pour le propriétaire du copyright dépasse 1 000 $.

Au Koweït le code de propriété intellectuelle a mentionné dans l'article 42: "*Est puni par une peine d'un an d'emprisonnement assortie d'une amende ne dépassant pas 500 dinars ou par l'une de ces deux peines:*

1 - Tout individu qui aurait violer les droits d'auteur mentionnés dans les articles 4,5 et 6;
2 - Tout individu qui aurait commercialisé, distribué ou publié, par tout moyen que ce suit un produit imité;
3 - Tout individu qui aurait rendu publics ou aidé à rendre publics des logiciels avant leurs publication;
4 - Tout individu qui aurait violé la protection d'un logiciel "

L'article rajoute que le tribunal a le pouvoir de confisquer tout produit informatique piraté aussi bien que les outils servant au piratage ou à la distribution de tels produits(27).

SECTION II: LES ATTEINTES AUX DROITS

Certaines informations circulant sur le réseau peuvent porter atteinte au droit de propriété des personnes **(A)**, à leur personnalité **(B)** et les atteintes à l'intégrité psychique **(C)**.

A) Les atteintes à la propriété

Nous avons vu que les contrefacteurs pouvaient utiliser Internet comme moyen de vente de leurs produits, en prenant l'exemple de la contrefaçon de logiciels. Il se peut également, que l'on diffuse directement sur le réseau une contrefaçon, ce qui peut également constituer l'infraction. En effet, "*La protection d'une œuvre se caractérise par une totale indifférence quant au support. Sur la question particulière de la*

(27) Art.42 C.P.I.K.

contrefaçon, seul le résultat compte, à savoir la reproduction ou la représentation publique d'une œuvre sans autorisation du titulaire des droits. Peu importe le procédé technique, le support utilisé (numérique ou non, en ou hors ligne) ou encore l'origine de la copie piratée. Le droit français est donc doué d'une faculté d'adaptation qui le place d'emblée au premier rang des lois applicables à Internet."[28] Celle-ci peut concerner la contrefaçon de marque par l'insertion de meta-tags frauduleux **(1)** ou une contrefaçon de marque par réservation de domaine **(2)**.

1) La contrefaçon de marque par l'insertion de "*meta-tags*" frauduleux

L'Internet peut être un fabuleux outil de communication. Cependant, ses possibilités conduisent à des évolutions antagonistes et parfois apocryphes, lesquels ont pour conséquences l'impossibilité d'atteindre l'information, la requête étant noyée dans une masse indistincte de données parasites. La publicité occupe par conséquent une place encore plus importante sur le réseau des réseaux, avec ces dérives habituelles (publicité mensongère, déloyales, etc.....). Mais apparaissent aussi des formes nouvelles, intrinsèques à l'Internet, d'infection liée à la publicité. Il s'agit de s'aider des formidables et indispensables guides que sont les moteurs de recherche et annuaires[29]. Les moteurs de recherche fonctionnent de diverses manières, leur robot plus ou moins évolué travaillant au niveau des mots-clefs choisis par le créateur du site Web ou directement sur tout ou une partie du texte de celle-ci. C'est alors qu'apparaît le concept de " meta-tag ": il s'agit d'un ou de plusieurs mots-clefs artificiellement ajoutés au contenu de la page, sans que cela soit perceptible pour le visiteur, mais influençant le comportement du robot qui analysera la page pour la référencer. En pratique, la création de meta-tags ne pose aucune difficulté; par exemple, puisque le langage HTML ne

(28) Prévenir les atteintes à la propriété littéraire et artistique sur Internet, **http://www.celog.fr/expertises**

(29) Un annuaire est un site de référencement hiérarchique organisé entièrement par des individus tandis qu'un moteur de recherche utilise un robot chargé de référencer automatiquement les sites suivant leurs mots-clefs; existent aussi des méta-moteurs de recherche, robots chargés de poser une requête simultanément à plusieurs moteurs de recherche et d'en synthétiser le résultat.

prendra en compte que le texte figurant entre les balises " < Body > " et " < /Body > ", il suffira d'ajouter ses mots clefs derrière cette balise.

En soi, le procédé n'a rien d'illégal. Bien entendu, cette promotion est un peu frauduleuse, mensongère, elle fausse le jeu normal de l'indexation des pages Web par le robot du moteur de recherche; mais ce n'est pas en somme très critiquable ni inquiétant comparé à d'autres agissements bien plus répréhensibles. On peut plutôt assimiler cette pratique à une sorte de coutume. Mais qu'en est-il quand les meta-tags utilisés sont des noms de marques ? La première affaire d'utilisation frauduleuse de meta-tags a eu lieu aux Etats-Unis, avec la décision Playboy(30): en l'espèce une ancienne salariée du magasine avait ouvert son propre site dans lequel étaient dissimulés les termes "playboy" et "playmate". En France, une action a déjà donné lieu à une interdiction provisoire dans l'attente d'un jugement au fond(31).

Les meta-tags frauduleux sont sans doute une forme relativement originale de contrefaçon de marque. D'autres modes de répressions sont envisageables, telle la concurrence déloyale(32) ou l'action parasitaire. Il faut cependant que certaines conditions soient remplies, les sites doivent apparaître comme concurrents. En l'occurrence, dans une certaine mesure, le site Web correspondant à la marque cachée frauduleusement dans le code source est privé d'un internaute, c'est-à-dire d'un consommateur potentiel, par le site utilisant le meta-tag frauduleux. Cependant, l'infraction de contrefaçon de marque, lorsqu'elle s'applique prévaut sur ces actions.

2) La contrefaçon de marque par réservation de nom de domaine

Pour faciliter la communication, les serveurs aux adresses numériques empruntent un langage plus clair. Mais la règle générale s'appliquant ici est très simple: " premier arrivé, premier servi"(33). Est

(30) THIEFFRY (P.), "*Les avancées des tribunaux américains dans le cybermonde: Playboy contre les meta-tags*", Les Echos, 19 janvier 1998.

(31) TGI Paris, ord. Réf., 4 août 1997, JCP (E) 1997 pan. n° 1021

(32) HAAS. M-E, "*Les meta-tags comme moyen de générer du trafic sur Internet et la contrefaçon de marques*"., Gaz. Pal.,30 juillet 1998, p.1020.

(33) FREDERIC-JEROME P., *La criminalité sur l'Internet*, Que sais-je, Puf, 2000, p.22

apparu alors très vite un problème majeur de parasitisme, du fait d'une course à l'enregistrement. En effet, le nom de domaine d'un site correspond à son adresse et revêt une importance particulière. Il est alors intéressant de prendre un nom de site Web proche d'un nom de site très connu ou du moins très visité, pour profiter des erreurs que peuvent effectuer les utilisateurs au moment d'y accéder. Imaginons simplement un URL ainsi construit: www.yaho.fr, imitant donc le célèbre annuaire dont l'URL est www.yahoo.fr. Des conflits d'autres types peuvent surgir; par exemple, l'appropriation d'un nom de marque par une société concurrente de la société exploitant la marque, ou l'enregistrement d'un patronyme, d'un lieu géographique, etc.... On a donc vu apparaître un véritable trafic international des noms de domaine, des individus revendant les noms qu'ils avaient pensés à enregistrer plus rapidement que les personnes concernées plus légitimement.

En France, l'autorité d'enregistrement chargée de l'attribution des noms de domaine portant le suffixe "fr" est l'AFNIC, (Association française pour le nommage Internet en coopération) gérée par l'INRIA (Institut National pour la Recherche en informatique et en automatique). Cet organisme a élaboré " une convention de nommage "[(34)] fixant des critères pour l'attribution du nom de domaine. On apprend ainsi que lorsque le nom est un nom de marque, le certificat d'enregistrement à l'INPI ainsi que son numéro doivent être fournis. Mais il peut arriver que sa vigilance fasse défaut et que cet organisme ne reconnaisse pas un nom de marque, dans le cas où la marque est déposée avant. Il y a alors contrefaçon de marque, à la condition toutefois, de respecter le principe de spécialité. La protection ne joue en effet que lorsque le nom est repris par une entreprise à l'activité similaire; à cela s'ajoute une exception en faveur des noms de marque notoires[(35)] dont la reprise est toujours considérée comme parasitaire.

(34) elle est disponible sur Internet à l'adresse suivante: http://www.nic.fr/Procedures/nommage.html.

(35) A contrario, TGI Paris, 23 mars 1999, Alice c/ Alice, sur legalis.net. En l'espèce, la SNC Alice (agence de publicité) n'était pas assez notoirement connue pour interdire à la SA Alice (logiciels) de créer un site web dont le nom est http://www.alice.fr.

De manière générale, donc, les noms de domaine ne posent pas de problèmes juridiques nouveaux[36], même si un contentieux fourni devrait se développer. Bien que ce ne soit pas la première en France, l'affaire Saint-Tropez[37] est la plus célèbre avec force de précédent[38]: une entreprise fut condamnée pour avoir déposé le nom de domaine "www.saint-tropez.com " alors qu'elle venait de réaliser pour le compte de la commune le site www.saint-tropez.fr " (le suffixe com signifie que l'entreprise l'avait déposé aux Etats-Unis, mais cela n'a pas arrêté le juge, dont l'intervention est étranger au lieu de dépôt). De même, la récente affaire SFR[39] démontre par l'ampleur des réparations exigées (1.000.000 F de dommages-intérêts) la volonté péremptoire du juge de moraliser les modalités d'obtention de nom DNS.

La jurisprudence sur le Minitel en France devrait s'appliquer par ailleurs par analogie, bien qu'au niveau technique, les différences quant à l'attribution des noms soient considérables. L'affaire Pamela[40] est à cet égard particulièrement intéressante: une première société avait déposé la marque " Pamela " en 1992 pour des services de communication télématique en classe 38; une seconde dépose la même marque pour des services de télécommunication, communication par terminaux d'ordinateur, communication radiophonique, transmission de messages télématiques ou téléphoniques en classes 35, 38 et 41. La règle en droit positif est que l'enregistrement de la marque ne confère à son titulaire un droit de propriété sur cette marque que pour les produits et services qu'il a désignés (L 713-1 C.P.I.F), mais la seconde entreprise se fait néanmoins condamner, les deux modes d'exploitation du terme Pamela étant similaires. Le juge a donc réaffirmé son attachement à la répression des abus suscités par l'appropriation de termes à des fins de publicité. En l'espèce, il en confond même télématique et Internet.

(36) Il n'existe pas d'antécédents judiciaires dans la jurisprudence Koweïtienne.

(37) TGI Draguignan, 21 août 1997, sur legalis.net

(38) Voir une affaire similaire, Référé TGI Versailles 22 octobre 1998, Marie d'Elancourt, sur Legalis.net.

(39) TGI Nanterre, 18 janvier 1999, accessible sur legalis.net.

(40) TGI Paris, 3eme Ch., 10 juin 1998, S.D.T. c/ EUREVA, sur Cyberlex, note M. RICOUART MAILLET.

Le droit commun répressif s'applique certes aux circonstances d'attribution des noms de domaine. Cet encadrement à posteriori et très lourd (des peines d'emprisonnement sont prévues) fait l'objet d'attaques des partisans de l'autorégulation, préférant un contrôle conventionnel par voie de clauses compromissoires et surtout par une analyse préventive accrue au moment du dépôt du nom de domaine(41). Mais l'autorégulation, efficace lorsqu'il s'agit de moraliser les commerces profitant de la vitrine Internet, ne peut répondre à elle seul à nombre de pratiques déloyales.

B) Les atteintes à la personnalité

Si Internet est à la fois expression d'un savoir-faire informatique et expression tout court, un type de délinquance plus spécialement regroupe les deux compétences, l'atteinte à la vie privée. En effet, si l'intrusion dans un système est souvent synonyme d'altération des données, celles-ci ne sont pas neutres, et peuvent recouvrir des points sensibles de la personnalité de la victime. L'atteinte à la vie privée est donc à la fois constituée par l'intrusion dans un espace intime, ce qu'on a déjà étudié sous l'angle du piratage, et par la diffusion de propos ou d'images appartenant à la vie privée, ce qui range l'atteinte à la vie privée dans la catégorie de la criminalité de type éditoriale. Cette ambivalence, voire cette ambiguïté, de la protection de la vie privée sur Internet se reflète dans les différentes qualifications applicables, tandis qu'est recherché un certain droit à l'anonymat et l'interdiction d'un " marché de la vie privée" par l'instauration d'une protection des données personnelles à l'individu. C'est sous cet angle là que l'on traitera du droit à l'image et à la voix en tant que propriété privée de chaque individu **(1)**. L'autre forme d'atteinte à la vie privée via Internet relève d'une infraction plus classique et plus répandue La diffamation **(2)**.

1) Le droit à l'image et le droit à la voix

Le droit à la vie privée est un droit fondamental, inhérent à toute démocratie. Il n'est donc pas lié à un quelconque support mais

(41) NAIMI M., "*La problématique des noms de domaine, ou l'attribution des adresses électroniques sur le web*", DIT 1997/2, p.8.

transcende la technique pour s'appliquer dès qu'une personne cherche à communiquer une information au public, par quelque moyen que ce soit.

Il est désormais commun de s'interroger sur une autonomie du droit à l'image, à la fois plus large que le droit au respect de la vie privée, puisqu'il englobe la vie publique de l'individu, et plus restreint, dans le sens où il ne concerne pas tous les aspects de la personnalité de l'individu, mais seulement les manipulations de son image. Internet s'inscrit donc dans cette logique générale, et la cyber-criminalité n'a pour seule spécificité ici que l'extraordinaire panel de moyens mis à la disposition de l'auteur de l'infraction; on parle de " techniques de morphing, mapping, de blue screen, d'incrustation, de mixage de sons/images réels et virtuels, d'altération des visages, d'imitation des voix, de truquage des scènes "[(42)]. (Récemment, un groupe d'individus a été arrêté en Egypte pour avoir trafiqué des photos de personnes célèbres pour un usage pornographique, à but lucratif sur Internet.)

Le droit pénal français, heureusement, inclut toutes ses possibilités dans une seule infraction, le délit de montage, prévu à l'art.226-8 N.C.P., alinéa 1°[(43)]: "*est puni d'un an d'emprisonnement et de 100 000 F d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention*".

Le procédé de publication de l'image ou de la parole d'une personne est indifférent et englobe donc l'Internet. La répression est plus restrictive que le serait une simple protection pénale du droit à l'image dans le sens où des exceptions, causes de non imputabilité, sont prévues lorsque le montage a été réalisé avec l'accord de la personne, lorsqu'il paraît évident, (cette notion devant sans doute s'apprécier de manière objective, par référence à l'appréciation qu'en ferait un " bon père de famille ") ou

(42) Rapport de la CNIL, "*Voix, image et protection des données personnelles*", Paris, la Documentation Française, 1996, p.48.

(43) Anciennement article 370 C.P.F, inséré par la loi n°70-643 du 17 juillet 1970

lorsque l'auteur a pris la peine d'indiquer au public qu'il s'agit d'une mise en scène.

Les règles juridiques générales au Koweït ne comportent aucun article incriminant la modification, trucage, montage d'images retransmises sur Internet.

La vie privée de l'individu est donc protégée indirectement dans son seul composant visuel ou sonore, mais surtout est sanctionnée dans l'esprit du texte la manipulation de l'information.

2) La diffamation, l'injure, la dénonciation calomnieuse

Il est très facile de mener une campagne de dénigrement grâce à Internet. Les mésaventures du ex- Président américain Bill CLINTON en sont le parfait exemple: il a suffit qu'un internaute diffuse sur son site personnel un article relatif à une maîtresse de Bill Clinton pour que 700 sites (fin janvier 1998) se consacrent au "*Monicagate*", que le reste de la presse s'empare de l'affaire, ce qui a failli aboutir à une procédure d'empeachement à l'encontre du président(44).

Internet risque d'ailleurs de développer ce type de comportement. Fausses rumeurs et accusations sont un excellent moyen de porter atteinte à une personne, qu'elle soit physique ou morale, d'autant plus que grâce à Internet elles peuvent être diffusées à travers le monde entier(45). Airbus Industrie a fait les frais de cette désinformation: des utilisateurs de *newsgroups* (visiblement leur principal concurrent) laissaient des messages agressifs à l'encontre de la société, laissant entendre que l'accident de l'A-320 d'Habsheim ne serait pas le dernier étant donné le peu de qualité du travail d'Airbus. De même, des Birmans résolument contre un chantier du pétrolier Total dans leur pays critiquent sur des *newsgroups* et des sites l'attitude de total, comparée à des "*néo-colonialistes cupides et sanguinaires*".

(44) "*L'étrange itinéraire médiatique d'un scandale*" Le Monde 25, 26 janv. 1998 -"*Sexe, mensonges et internautes*" Le Monde, supplément multimédia 16,17 août 1998

(45) J. GUISNEL, *Guerres dans le cyberespace*, éd. La Découverte, p. 231 & s. - " Les guérilleros du XXIème siècle " Le Monde supplément Multimédia 23,24 août 1998

Les contre-sites *("horror sites")*, détournant le contenu de certains sites, s'il se contentent la plupart du temps d'être parodiques, peuvent également être plus virulents(46).

L'application des dispositions de la loi du 29 juillet 1881 et notamment l'art. 29 serait un moyen de lutter contre ce type de propos.

Ces dispositions ont même vocation à protéger les personnes morales(47), dès lors que l'attaque ne se constitue pas de dénigrement des produits, des services ou des prestations offerts par la personne morale(48).

Si les faits, inexacts, reprochés sont susceptibles d'entraîner des sanctions judiciaires, administratives ou disciplinaires et surtout si leur dénonciation est faite par Internet à une autorité compétente (sur les messages laissés sur le site de cette autorité, par e-mail), l'auteur des reproches pourrait être poursuivi sur le fondement de dénonciation calomnieuse, sanctionnée par l'art. 226-10 C.P.F.

On peut rapprocher de ces infractions, une autre infraction basée également sur le mensonge, même si elle n'a pas pour objet de porter atteinte à une personne, mais plutôt d'en enrichir une autre: l'art. 10.1 de l'ordonnance du 28 septembre 1967 puni de 2 ans d'emprisonnement et de 10 millions d'amende le fait pour toute personne de répandre sciemment dans le public des informations fausses ou trompeuses en matière boursière(49).

Le C.P.K ne comporte pas d'articles incriminant la diffamation et l'injure sur Internet, mais nous voyons que la publication sur ce moyen de communication (sur des sites ouverts au publics) de tout ce qui porte atteinte à la vie privée d'un individu, peut être considéré comme diffamation ou injure, normalement incriminées par la loi.

(46) "*A l'attaque des world companies*" Le Monde Cahier Multimédia 1er/2 mars 1998
(47) Crim.12 oct. 1976 Bull. Crim. n°287
(48) Crim. 8 fév. 1994 Bull. Crim. n°58
(49) " Les délits boursiers sur l'Internet ", Les Echos, 18 déc. 1997

C) Les atteintes à l'intégrité psychique

Les menaces sont les dernières infractions que nous étudierons dans ce chapitre. Internet constitue le moyen idéal pour celui qui a l'intention de menacer quelqu'un: il lui garantit, a priori, un anonymat complet, tout en lui permettant de s'exprimer de façon privée (par un e-mail) ou publique (sur un site Web). La presse nous informa récemment qu'un jeune américain avait menacé de mort par courrier électronique 59 étudiants d'une faculté qui l'avait renvoyé(50).

Le droit pénal français appréhende de façon complète les divers comportements menaçants. Il les distingue selon deux critères: selon que la menace porte sur la commission d'une infraction contre les personnes(51) (un crime ou un délit) ou sur la commission d'une infraction contre les biens(52) (une destruction, dégradation ou détérioration d'un bien), et selon que la menace est simple ou émise sous condition.

Dans ce cadre, les droits Koweïtiens et français se rejoignent étant donné que l'écriture peut constituer une forme de menace. Ainsi trouve tout dans l'article 222-17 du C.P.F que la menace peut être: "*matérialisée par un écrit, une image ou tout autre objet*". De la même retrouve-t-on dans le C.P.K l'article 173 citant que: "*tout individu qui aurait menacé un autre en sa personne, réputation ou biens (...) que ce soit oralement ou par écrit*...". Certes cela peut être applicable à toute menace envoyée par e-mail.

SECTION III: LES ATTEINTES A LA SOCIETE

Internet est un moyen privilégié de communication et d'échange pour les délinquants étant donné qu'il peut représenter de nombreux atouts pour la transmission d'informations relatives à leurs activités criminelles.

Mais cette atteinte peut concerner non seulement une société tout entière, mais des individus (notamment mineurs) pouvant être la cible de

(50) " Internet au bord de la crise à cause d'un tueur virtuel " Marianne n°42 9-15 fév. 1998
(51) Art.222-17-18 du C.P.F.
(52) Art.322-13 du C.P.F.

messages à caractère sexuel explicite pouvant les choquer. De ce fait, il est indispensable de trouver les moyens de protéger la société, de certains messages comme ceux présentant un moyen idéal de communication pour les organisations criminelles **(A)**, et à caractère sexuel pouvant affecter les mineurs **(B)**.

A) la messagerie et le crime organisé

Tout d'abord, le caractère international du réseau leur garantie une communication sans frontières, à la dimension des groupements organisés de criminels d'aujourd'hui. Ceci contribue d'ailleurs à la coopération de plus en plus importantes des différentes mafias.

De plus, l'instantanéité, ainsi que la possibilité d'échanger des informations sous différentes formes (images, sons, textes, fichiers..) qu'offre Internet en fait un moyen de communication plus intéressant que le courrier traditionnel, le téléphone ou le fax. La probabilité de contrôle de leurs échanges est également infime, compte tenu du nombre d'informations qui circulent sur le réseau.

Enfin, quand bien même leur correspondance serait interceptée, les techniques de cryptologie(53) utilisables sont multiples et efficaces. Elles sont multiples du fait de la multiplicité des supports de l'information. La méthode la plus répandue est le chiffrement d'un texte en un langage codé où chaque chiffre ou lettre en représente une autre. Cette technique fort ancienne connaît un essor considérable en raison de la possibilité de combiner les lettres (minuscules et majuscules), chiffres et symboles, et de l'existence de logiciels capables de créer des principes de chiffrement extrêmement complexes. Bien mieux, la sténographie(54) présente l'avantage de ne pas éveiller les soupçons sur le document codé. Ce dernier est une image. Chaque image en informatique est composée de pixels, des minuscules points de couleur, dont cette dernière est déterminée par un chiffre. En modifiant quelques-uns de ces chiffres

(53) La cryptologie "*permet de verrouiller des données à l'aide d'un mot de passe ou d'un système intégré de façon à empêcher un tiers non autorisé d'avoir accès aux données ou de les reproduire*".

(54) S. LE DORAN & P. ROSE Les cyber mafias, éd. Denoël, p. 60; D. MARTIN, *La criminalité informatique*, éd. PUF p. 42

par d'autres, selon un code préétabli (chaque chiffre représentant une lettre), l'on modifie de façon imperceptible les couleurs de l'image. Le destinataire relève alors les pixels qui ne sont pas de leur couleur initiale, traduit les chiffres qui les représentent en lettres et déchiffre ainsi le message. Ces techniques sont également efficaces car si les autorités judiciaires parvenaient à intercepter l'un des messages codés, elles auraient beaucoup de difficulté à le décoder dans la mesure où les algorithmes sur lesquels repose le chiffrement peuvent être extrêmement difficiles à découvrir. De plus, les autorités de police ont beaucoup moins de moyens financiers et matériels que la criminalité organisée dont les profits lui permettent de s'assurer des meilleures techniques.

Grâce à ce moyen de communication, les délinquants peuvent préparer certaines des infractions qu'ils projettent de commettre, se rencontrer dans le but de participer à une même opération illicite. Les groupes terroristes, les mafias, les trafiquants sont les délinquants qui usent majoritairement de ce mode de communication entre eux. Ainsi, les autorités américaines ont découvert qu'un groupe de narcoguérilleros avait contacté via Internet, en 1997 d'autres cartels pour les inviter à une réunion sur les problèmes liés à la production, à la commercialisation et à la consommation de cocaïne(55). De la même manière, il fut découvert en 1995 que la mafia ukrainienne tentait d'indiquer à la mafia calabraise le moment et le lieu d'une livraison d'héroïne en lui envoyant une photo codée par Internet(56).

Ce type de message tend à permettre la commission d'une infraction, à laquelle participeront nécessairement plusieurs personnes puisque sa préparation implique une correspondance entre au moins deux individus. Dès lors, nous devons nous demander si ces messages seraient susceptibles de constituer un élément constitutif d'une association de malfaiteurs.

L'art. 450-1 C.P.F énonce que "*constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation,*

(55) S. LE DORAN & P. ROSE, *Les cyber mafias*, éd. Denoël, p.44

(56) D. MARTIN, L*a criminalité informatique*, éd. PUF, p.42

caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis de dix ans d'emprisonnement". L'art. 212-3 C.P.F. incrimine de façon spécifique l'association de malfaiteurs créée dans le but de commettre un crime contre l'humanité afin de prévoir une peine plus importante que celle de droit commun. Les associations en matière de terrorisme font également l'objet d'un texte spécifique (art. 421-2-1 C.P.F) puisque parmi les actes terroristes, certains sont des crimes ou des délits punis de 10 ans d'emprisonnement tandis que d'autres sont des délits punis de moins de dix ans d'emprisonnement. Cela permet de plus de les sanctionner plus lourdement. Enfin, l'association de malfaiteurs ayant pour but de porter atteinte aux systèmes de traitement automatisé de données est exceptionnellement incriminée, alors qu'elle concerne des délits punis au maximum de 3 ans d'emprisonnement(art.323-4 C.P.F).

Si nous partons du principe que les auteurs de ces messages constituent des organisations et que leur but est de commettre les infractions citées plus haut, comme nous pouvons le penser de groupes terroristes ou de mafias, la question devient de savoir si la communication interceptée caractérise suffisamment la préparation. La réponse à cette question sera inhérente au contenu de la communication. La Chambre Criminelle de la Cour de Cassation Française a admis en 1990[(57)] comme acte préparatoire constituant une association de malfaiteurs une conversation téléphonique au cours de laquelle les accusés décidaient de reporter la date de commission d'un vol et l'un d'eux proposait un véhicule pour en faciliter la commission. Nous pouvons donc penser qu'une communication, quelque soit la forme, via Internet pourrait constituer un acte préparatoire déterminant. La lutte contre le crime organisé n'a pas été mentionnée en droit Koweïtien. Cependant nous pouvons mentionner dans ce cadre le pacte criminel, incriminé par l'article 56 du C.P.K. auquel peut être assimilés les accords criminels passés sur Internet. Cependant il n'existe pas de mécanisme défini pour l'incrimination des correspondances entre les membres de l'organisation criminelle.

(57) Crim. 20 fév 1990 D.1991 Juris. P.395

En conclusion. Notons les remarques suivants: La première est que l'incrimination d'association de malfaiteurs et son interprétation par les juridictions françaises constitue un atout dans la lutte contre la criminalité organisée internationale et une réponse aux difficultés d'application du droit à un phénomène transfrontière comme Internet. En effet, la jurisprudence(58) considère que la loi française est applicable et les juridictions françaises sont compétentes dès lors que l'un des actes préparatoires ou une des infractions envisagées a été commis en France.

Cette lutte contre la criminalité organisée sera d'autant plus efficace que désormais, depuis la loi du 17 juin 1998(59), les personnes morales peuvent être déclarées pénalement responsables de l'infraction (art. 450-4 C.P.F) et encourent ainsi la dissolution.

De plus, l'on peut noter que lorsque les autorités de police auront réussi à intercepter et à déchiffrer ces messages, l'utilisation de la cryptologie se retournera contre les malfaiteurs. Effectivement, la cryptologie permet d'identifier de manière quasi-certaine l'expéditeur ou le destinataire du message puisque la clé de chiffrement doit demeurer secrète.

B) les messageries à caractère sexuel

La diffusion de messages à caractère sexuel(60) est sans doute le principal vice que les médias ont retenu d'Internet. Il est vrai que ce moyen de communication a été très tôt découvert notamment par ceux qui font de la sexualité leur fond de commerce.

Le plus grand danger fut représenté comme celui des forums de discussions où les images pornographiques, souvent concernant des enfants pouvaient s'échanger sans aucune difficulté ni contrôle. L'ampleur du danger est cependant difficile à cerner: Une enquête de

(58) Crim. 20 fév 1990 D.1991 Juris. P.395 - TCorr Paris 16 oct 1991 Gaz. Pal. 1992.I. somm.46

(59) L. n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs - J.O. 18 juin 1998 p. 9255

(60) " Pornography on the Internet " Yaman Akdeniz **http://www.argia.fr/lij**; OTTAVIO FRANCESCON " Les nouvelles techniques de l'information et de communication et leur exploitation à des fins illicites: l'exemple des activités touchant à la pornographie dure dans l'Internet ", Rev. Int. de Criminologie et de Police, 1996, n°1, p. 61

Time Magazine[61] révéla en 1995 que 83,5 % des forums comprenaient des images pornographiques tandis qu'une autre étude[62], moins controversée, ne parle que de 0,3% des forums.

De plus, contrairement à l'image désormais répandue, découvrir une image pornographique par surprise devient de plus en plus rare. Le nom du site ou du *NewsGroup* sera souvent révélateur et certains d'entre eux indiquent sur leur page d'accueil un avertissement concernant leur contenu, demandent l'âge de l'utilisateur (il est vrai que cette précaution semble dérisoire) ou demandent le numéro de carte de crédit.

Nous avons vu qu'il existe de nombreux serveurs ou forums dont l'objet principal est la sexualité, sous quelque forme que ce soit[63]. Ceux-ci diffusent des images, des films pornographiques, proposent à la vente du "matériel". Certains *IRC* permettent des discussions érotiques..

La mise en œuvre d'un contrôle familial des informations accessible aux mineurs via l'Internet est néanmoins devenue possible grâce à des moyens logiciels ou des sociétés de services assurant le filtrage des sites ou informations directement consultables par un mineur connecté au réseau *(Net Nanny, Surf Watch, cybersitter)* certains sites lui seront ainsi interdits, à moins qu'il n'entre un code détenu par les parents et permettant l'utilisation intégrale des ressources de l'Internet.

CHAPITRE II
LES CYBER CRIMINELS

Le terme pirate dans l'inconscient collectif évoque des images fortes et tout au moins des sentiments troubles. A l'origine circonscrits dans le domaine maritime, les pirates ont évolué vers les airs et les routes, puis,

(61) Philip ELMER-DEWITT "*On a screen near you: Cyberporn*", Time, 3 juillet 1995, pp. 34-41; d'après une enquête Marty RIMM "*Marketing Pornography on the Information Superhighway*", 1995 Georgetown Law Journal 83, 1839-1934.

(62) Par MM. HOFFMAN et Novak - **http://www2000.ogsm vanderbilt.edu/rimm.cgi.**

(63) Quelques exemples de forums relatifs à la sexualité à connotation: scatologique " alt.binaries. pictures. erotica. tasteless " - nécrophile " alt.sex.necrophilia " - zoophile "alt.sex.zoophilia"

enfin, les info-routes[64]. Le concept renvoie de manière vague à une transmission, une communication ou un simple déplacement, détournés de leurs fins de manière inattendue. Ce détour par l'histoire semble en apparence garder tout son sens, car aujourd'hui comme hier, on distingue les pirates "free-lance", dont on peut dire en forçant l'anachronisme qu'ils sont plus ou moins anarchistes, des corsaires, vendus à une grande puissance.

Les premiers cherchent à s'approprier sans vergogne toute donnée transitant sur Internet, les seconds, de manière plus subtile, obéissent à un objectif de marketing, souvent en contradiction avec les impératifs de la protection de la vie privée. Mais cette distinction suivant le but plus ou moins mercantile est surtout théorique et fausse du point de vue sociologique et juridique! Même les *hackers* (pirates) indépendants cherchent à produire de l'argent, en mettant à la disposition du public de sites Internet "*warez*" financés par la publicité, ou encore en procédant au chantage.

Or, dans le cadre de l'incrimination du comportement frauduleux du *hacker*, le danger réside dans une dépendance du droit envers les nouvelles technologies. Il faut donc éviter les textes trop précis pour qu'ils ne soient pas caducs dès leur adoption, et aussi respecter le principe "*nulla poena sine lege*", impliquant le refus de lois trop générales, ce qui serait attentatoire aux libertés. Ainsi, par recherche d'un consensus, le législateur aussi bien que les instances communautaires ont produit une multiplicité de textes souvent délibérément obscurs, pour permettre à la jurisprudence de faire acte de création prétorienne.

Les cyber criminels des temps modernes plaisent au public, qui lui associe des qualités héroïques telles que la bravoure, la ruse ou la compétence. Certes, ces pirates ont à leur crédit le fait qu'il n'y ait pas de sang versé, pas de danger physique, leur emploi du temps ressemble à

(64) Le taux de piratage de logiciel au monde a atteint 40% pour l'année 1999, affectant l'industrie informatique 574 millions de dollar, en Europe d'est ce taux s'élève à 77% alors qu'en Afrique et Moyen-Orient il a atteint 65% contre 62% en amerique latine, 39% en Europe occidentale et 28% seulement en Amérique du nord; Al-Qabsse, 12 /10/1998, p.17.

première vue à un exercice cérébral. On a vite fait à chaque découverte dans le domaine de la sécurité de proclamer systématiquement qu'il ne tiendra pas longtemps devant le "*génie inventif des hackers*". La réalité est sans doute moins heureuse: cette imprévisibilité des pirates accentue un sentiment de peur parmi les gérants de systèmes, ce qui permet de comparer certaines de leurs pratiques à du terrorisme, bien que se développent de plus en plus des règles légales et jurisprudentielles visant à réprimer le piratage.

Nous tenterons dans ce qui suit de traiter des auteurs des crimes informatiques **(Section I)**, leurs techniques **(Section. II)** et leurs motivations **(Section. III)**.

SECTION I: LES AUTEURS DES CRIMES

Le réseau est un formidable outil d'échange de l'information. Cependant, certaines des informations sont destinées à n'être consultées que par des individus particuliers. Il faut protéger la confidentialité et l'intégrité de ces informations contre de nombreuses attaques.

Par fraude informatique, on entend non seulement la délinquance assistée par ordinateur, mais également les atteintes matérielles (vol, sabotage) au matériel informatique. Ces dernières ne nous concernent pas, mais il est intéressant de relever qu'elles deviennent de plus en plus nombreuses et représentent des sommes de plus en plus importantes(65).

Nous nous attacherons à la délinquance assistée par ordinateur (Commise par une génération de techno-criminels face auxquels les systèmes répressifs nationaux demeurent bien souvent impuissants). Celle-ci a pour objet les données, c'est-à-dire l'information, qui est contenue par un ordinateur ou qui circule sur un réseau. Elle fait de plus en plus l'objet d'attaques afin de porter atteinte à sa confidentialité ou à son intégrité.

(65) "Au poids, les composants électroniques valent aujourd'hui plus cher que de l'or ou de la marijuana. " Commissaire D. PADOIN," *Cyber-Criminalité: la loi du silence*", Le Figaro, 29 nov. 1997

L'explosion des micro-ordinateurs dans les années quatre-vingt créa un nouveau type de délinquant: le "pirate" informatique. L'originalité et l'impact de ses pratiques(66) poussa les criminologues à s'intéresser aux motivations des délinquants informatiques(67). Ce sont ces mêmes motivations que l'on retrouve chez les fraudeurs utilisant le réseau puisque ce type de délinquance n'est que la forme la plus actuelle de la délinquance informatique. La seule innovation en la matière relève du vocabulaire. Les véritables pirates utilisent habituellement un modem ou un autre dispositif de transmission pour découvrir un code machine ou un mot de passe et s'introduire ainsi illégalement dans un ordinateur afin d'y opérer un véritable cambriolage électronique. Les finalités de ces intrusions sont diverses: vol ou destruction de données, de programmes ou encore introduction au sein de l'ordinateur ciblé de programmes destructeurs ou désorganisation (virus, vers, cheval Troie).

A la suite des "*phreakers*"(68) qui utilisaient le téléphone pour se connecter aux ordinateurs, sont apparus les "*hackers*"**(A)** et les "*crackers*"**(B)** qui eux agissent par le biais d'Internet. Dorénavant, 80 % des connexions pirates(69) utilisent ce support. Ces pirates, s'ils emploient les mêmes méthodes, ne poursuivent pas les mêmes buts.

A) Les *hackers*

Le terme de *hacker* désigne, à l'origine, "*une personne qui aime comprendre et utiliser les finesses techniques des programmes. Il qualifie aussi aujourd'hui les délinquants pénétrant par effraction dans des sites informatiques*"(70). Les *hackers* sont principalement des adolescents

(66) Le film " Wargame " contribua à la publicité de ces pratiques en s'inspirant du piratage par un jeune américain, Kevin MITNICK, des systèmes du Commandement de l'Armée de l'Air américaine.

(67) P. ROSE, *La criminalité informatique*, éd. PUF, 1988; C. JAN & G. SABATIER, *La sécurité informatique*, éd. Eyrolles, 1989

(68) Du verbe "*to freak*", " faire flipper ": dans leur langage, les "*f*" sont remplacés par "*ph*", soit les premières lettres de leur outil, le téléphone "*phone*"

(69) Selon un enquête du FBI - *Guerres dans le cyberspace* J. GUISNEL, éd. La Découverte / Poche 1997

(70) René TREGOUET, des pyramide du pouvoir aux réseaux de savoirs, Rapport d'information, 331-1997/98, commission des finances, Senat.

(étudiants ou lycéens) ou de jeunes personnes privées d'emploi. Une étude menée en 1994 par le *Federal Bureau of Investigation* FBI estime que la majorité des *hackers* les plus dangereux sont âgés de 18 à 35 ans, même s'il n'est pas exceptionnel qu'ils soient beaucoup plus jeunes.

Ces pirates n'ont aucune intention frauduleuse. Comme leur nom l'indique, ils ont pour but de s'introduire dans des ordinateurs distants, mais dans un esprit simplement ludique. Leur motivation n'est que le jeu, voire le défi. On les décrit généralement comme des gens jeunes, ayant souvent des compétences en matière informatique, respectant un code de l'honneur et d'une grande patience(71). Ce sont des "entrepreneurs" selon la classification de Philippe ROSE(72), dont l'un des divertissements est de percer les divers types de systèmes de protection qui peuvent exister avant de laisser un "souvenir" à leur victime afin de lui indiquer leur attaque.

Il apparaît que l'activité du *hacker* peut être classée en trois catégories(73). Plus exactement, le terme de pirate regroupe trois types de personnes qui parfois n'ont que peu de points communs. Les premiers s'intéressent aux failles méconnues logées dans la structure même d'Internet, pour le cas échéant, les exploiter. Sont ici de manière spécifique seuls concernés l'Internet et les réseaux intranet (système interne utilisant les structures d'Internet pour relier différents ordinateurs entre eux; cette compatibilité avec Internet est dangereuse puisqu'il suffit qu'un seul ordinateur dispose d'une connexion Internet, et cela ouvre une " porte " vers tous les terminaux du réseau intranet)(74).

Dans une autre acceptation commune du terme pirater est visé le comportement cherchant à s'approprier toute chose possédant une valeur marchande: logiciels, musique, etc... autant de faits illicites que le

(71) Note du Service central de la sécurité des systèmes d'information du 28 mars 1994, " Le créateur de virus en jeune homme ordinaire ", Courrier International, 29 janv. 1998

(72) P. ROSE, *La criminalité informatique*, éd. PUF, 1988, p.69

(73) La moyen d'age des pirates de l'informatique au Koweït est de 15 à 25 ans, Al- Qabass, 3 /6/ 2000, p.12.

(74) L'Internet est devenu un réseau de prédilection pour le hacking, selon une étude menée en 1995 par Sun Microsystems, entre 80% et 90% des attaques logiques menées contre des systémes informatiques sont opérées via l'Internet.

législateur a rassemblés sous l'unique prévention de contrefaçon. Le cyberespace dans ce cas de figure est toujours un territoire de choix pour la réalisation de ces divers méfaits, mais il ne peut plus être envisagé de manière autonome. Il s'accompagne d'un dispositif " off-line ", pour, par exemple, " craquer " ou " déplomber " le logiciel, c'est-à-dire retirer ses protections.

Dans un troisième temps, le pirate s'occupe de la transmission du produit ainsi transformé par le biais de sites *Warez*; souvent, il hésite lui-même, par peur des sanctions pénales, à communiquer directement et notoirement ces réalisations. Aussi, sa recherche de protection le conduit naturellement à user et surtout abuser de liens hypertextes.

Généralement, le choix de la victime n'est pas non plus innocent. Même si aucune véritable intention malveillante ne les fait agir, les systèmes attaqués seront ceux d'une administration ou d'une société à laquelle il serait valorisant de s'affronter, soit parce qu'elle se vante de repousser toute attaque, soit parce qu'elle défend des valeurs que repoussent les pirates. Ainsi, la police mit fin en 1995 aux intrusions d'étudiants de l'EPITA (Ecole Pour l'Informatique et les Techniques Avancées) sur les serveurs d'universités françaises, de Thomson, du Pentagone, de l'US NAVY. Ces sites font partie de ceux qui font régulièrement l'objet d'attaques. Le département américain de la Défense a lui-même avoué avoir fait l'objet de 250 000 attaques en 1996(75). Certaines d'entre elles ont été menées par le pirate israélien " Analyser " qui aurait à son actif 1000 intrusions d'ordinateurs différents et qui a été arrêté en mars 1998(76). On peut même accéder sur Internet à un musée des meilleurs piratages d'un groupe de "*hackers*"(77) sur lequel figure entre autre celui du site de la CIA, rebaptisée à l'occasion "Central

(75) "*Le Pentagone encore visité par les hackers*" Le Monde Informatique 6 mars 1998; 250 000 attaques également en 1995 "*Guerres secrètes sur Internet*" Le Figaro, 21 nov. 1996; "*La cyber-flibuste, vent en poupe*" Le Figaro, 5 déc. 1997

(76) "*L'Analyseur, cambrioleur informatique, devient un héros d'Internet*" Le Monde, 28 mars 1998 p.1 "*Ehud Tenenbaum, pirate et héros*" Le Monde, supplément multimédia 19,20 juillet 1998

(77) http://www.dis.org

Stupidity Agency" et où figurent insultes et liens hypertextes avec des sites pornographiques.

B) Les *crackers*

Les "*crackers*" ont détourné les techniques développées par les "*hackers*" à des fins plus matérielles. Parfois, on les appelle "araignées" *("spiders")* car "*ils se cachent dans l'ombre, laissent des traces déplaisantes de leur passage et peuvent être dangereux*"[78].

Ils sont d'autant plus dangereux qu'ils s'échangent leurs techniques au sein de *newsgroups* spécialisés ou par l'intermédiaire de revues[79] distribuées par *mailing lists*. Ils vont même jusqu'à former des clubs tel le Chaos Computer Club de Hambourg[80] ou le CLODO en France (Comité Liquidant Ou Détournant les Ordinateurs). Désormais, ils représentent 90% des attaquants.

Les "agressifs"[81] agissent par vengeance personnelle ou professionnelle. Rare n'était pas l'hypothèse, du temps de la "simple délinquance informatique", de l'employé qui laissait un virus ou une bombe logique dans la mémoire de l'entreprise qui l'avait licencié. Cette possibilité s'offre désormais avec plus de facilité à celui qui sait utiliser Internet.

Les "*crackers*" peuvent également agir dans des buts stratégiques, idéologiques, terroristes ou cupides pour reprendre la classification établie par le Service central de sécurité des systèmes d'information.

- **L'attaque stratégique:** Des organismes gouvernementaux ou para gouvernementaux recherchent à obtenir divers renseignements (du secret-Défense aux renseignements industriels, militaire[82], diplomatique..) relatifs à certains Etats, ou ils peuvent attenter au

(78) *La bible Internet* Ed. Krol (traduction P. Cubaud & J. Guidon) coll. Guide & Ressources éd. O'Reilly international Thomson, 1995

(79) " Phreack ", " 2600 ", " Computer Underground Digest"

(80) Qui, en 1986, pénétra dans plus de 135 réseaux dans 9 pays industrialisés.

(81) P. ROSE, *La criminalité informatique*, éd. PUF, 1988, p.69

(82) Durant la guerre du Golf, l'armée américaine a révélé qu'un groupe de *hackers* hollandais s'était proposé de se mettre au service de l'action irakienne pour désorganiser le déploiement militaire américain moyennant la somme de 1 million de dollars.

fonctionnement des systèmes d'information de ces Etats. Ainsi, les Etats-Unis auraient consacré en 1996 au moins 30 milliards de dollars au financement de leurs organismes d'espionnage(83).

Des entreprises agiront de même à l'égard de leurs concurrents. Ainsi, on peut citer l'exemple(84) de l'entreprise qui intercepte les e-mails par lesquels son concurrent répond à des appels d'offres, ce qui lui permet de conclure les contrats en proposant des offres plus intéressantes.

- **L'attaque idéologique:** Les "crackers" peuvent agir pour défendre une opinion, qu'elle soit politique, religieuse, économique et se manifester à l'encontre de leurs opposants(85). De plus, "*il existe des courants de pensée qui mettent en avant le fait que l'information doit être libre et ne peut en aucun cas être la propriété d'une personne, d'un groupe, d'une organisation ou d'un Etat. Cette vision du monde est partagée par de nombreux pirates*". C'était le cas du Chaos Computer Club qui fit parler de lui dans la fin des années 80. Ce groupe revendiquait "*la reconnaissance d'un nouveau droit de l'homme, le droit à une communication libre, sans entrave et sans contrôle, à travers le monde entier, entre tous les hommes et tous les êtres doués d'intelligence, sans exception*"(86). Fin 1997, on a craint une telle attaque(87): un pirate se cachant sous le pseudonyme de Pants/Hagis annonça que "*tous les internautes qui ont lu une page de Yahoo et qui ont utilisé son moteur de recherche*" portaient "*une bombe logique enfouie dans les profondeurs de leur ordinateur*". Celle-ci devait activer un virus le 25 décembre 1997, si le gouvernement américain ne donnait pas l'ordre de libérer Kevin MITNICK, le plus célèbre des "pirates". Heureusement, cette menace s'avéra fausse. D'autres pirates ont, pour la même raison, pris le contrôle du site du journal

(83) P. ROSE, "*Délinquance informatique, info routes et nouvelle guerre de l'information*", Cahiers de la Sécurité Intérieure, n°24

(84) "*Cyberwars: la montée du crime informatique*" Les Echos, 10 fev 1998

(85) Durant la guerre du Kosovo, les responsables de l'OTAN furent scandalisés quand des *crackers* serbes ont réussit à infiltrer le réseau informatique de l'organisation pour y remplacer le Logo de l'OTAN par celui de la république serbe, Al Qabass, 3/6/2000, p.12.

(86) " Programme de base " du Chaos Computer Club en février 1984 dans "*La fraude informatique*" G. CHAMPY éd. Presses Universitaires d'Aix Marseille, 1992, p. 144

(87) "*Pants/Hagis, le pirate de Noël menace Internet d'une bombe à retardement*" Le Monde 12 déc 1997

le *New York Times* un jour de consultation importante[88]. C'est également pour des raisons idéologiques que certains Espagnols saturent les sites Internet de l'organisation séparatiste basque ETA[89].

- **L'attaque terroriste:** Leurs auteurs tentent de déstabiliser l'ordre établi par des attaques spectaculaires[90].
- **L'attaque cupide:** Elle a pour but d'entraîner directement, soit l'enrichissement de l'attaquant, soit l'appauvrissement de la victime.

Evidemment, toutes ces motivations peuvent s'ajouter les unes aux autres, ce qui rendrait difficile la stricte classification d'un comportement dans une catégorie.

La recherche du gain demeure tout de même la principale motivation. Cette dernière peut pousser un pirate à détourner directement de l'argent, ce que firent récemment des "pirates" russes en modifiant à leur profit (soit 3 millions de dollars) le système de transfert de fonds de la première banque américaine. Mais la principale forme de détournement est désormais celle de l'information. Cette tendance est si marquée que l'on parle de "Guerre de l'information" *("Information Warfare")*. Les délinquants veulent obtenir des informations pouvant leur procurer directement de l'argent, tels des numéros de cartes de crédit dérobés sur des serveurs commerciaux (notamment grâce à un logiciel appelé *Sniffer*)[91]. L'information en elle-même devient également l'objet de ces détournements: les entreprises, les administrations, les organisations de types mafieuses se livrent à de l'espionnage ou du sabotage pour obtenir des renseignements sur les particuliers ou sur leurs concurrents ou pour leur porter atteinte.

(88) "*Les pirates du cyberespace s'emparent du New York Times*" Le Monde, 16 sept 1998

(89) Le Monde, 26 nov. 1997

(90) Cette attaque a souvent un fondement idéologique. Ex: "*Cyberattentat par les Tigres de la libération de Tamil Eelam*" (informations de mai 98 **http://www.legalis.net**)

(91) pour exemple, Kevin MITNICK déroba 20 000 numéros de cartes de crédit en 1992 à la société NetCom, un groupe de pirates" bulgares acheta pour 100.000 dollars de marchandises après avoir dérobés des numéros de cartes de crédit (Le Monde - 25 nov. 1997); "*tarfic sur la toile*" Le Monde supplément multimédia, 21,22 juin 1998

SECTION II: LEUR TECHNIQUE D'ATTAQUE

Ces pirates se fondent sur deux "postulats de la délinquance informatique "[92] pour agir:

- Tout système informatique et de télécommunications comporte au moins une faille;
- Quiconque a accès à un système d'information est susceptible de découvrir ces failles.

L'intrusion pourra prendre diverses formes[93] Il s'agira:

- De s'introduire dans un système simplement pour prendre connaissance des informations qui y figurent et éventuellement de les copier ou de les "rapatrier" (en les effaçant du système visité) sur son propre ordinateur.
- D'introduire un programme informatique qui
- Transmettra toutes les données;
- Déclenchera à distance un programme résident intrus.
- De modifier des fichiers

Différentes techniques, plus ou moins agressives, peuvent être utilisées pour obtenir ou altérer des informations[94]:

- **Le déguisement**
- **La fouille**
- **Le cheval de Troie - Il** s'agit d'insérer un programme pirate dans un programme normal. Ce programme qui va permettre de rapatrier le mot de passe de l'utilisateur ou de détruire les fichiers de l'ordinateur destinataire est inclut dans un programme inoffensif.
- **Le salami / le saucisson** - C'est une technique qui consiste à multiplier les opérations, chacune d'entre elles étant imperceptible

(92) P. ROSE, "*Délinquance informatique, info-routes et nouvelle guerre de l'information*", Cahiers de la Sécurité Intérieure n°24

(93) "Attaques par les données " I. VASSILEFF **http://www.grolier.fr/cyberlexnet**; "La menace et les attaques informatiques " note du 28 mars 1994 du S.C.S.S.I

(94) A titre " pédagogique ": "*Les hackers après intrusion dans un système connecté: effacer ses traces.*", "Comment bloquer un serveur connecté à Internet?" **http://www.grolier.fr/cyberlexnet**

- **L'action asynchrone** - L'idée est la même que celle qui gouverne le salami, à la différence près que dans l'action asynchrone, le pirate agit une seule fois et prévoit une exécution non simultanée des instructions.
- **La bombe logique** - C'est un programme qui s'exécutera lors d'un événement prédéterminé par le programmateur. Ses conséquences peuvent être minimes (un message s'affiche) ou importantes (destruction des fichiers). La menace de Pants/Hagis était une bombe logique qui devait se déclencher le jour de Noël.
- **Le virus** est un petit programme ayant pour finalité d'altérer, d'endommager ou de détruire un système informatique, les virus peuvent facilement s'accommoder de tout type de support (disquette, disque dur, CD-Rom, voire mémoire ordinateur) Il existe près de 12 000 virus dans le monde PC, 6 nouveaux étant créés par jour(95).

  On distingue les virus selon leurs effets(96):
- les effets ludiques, animations sonores ou graphiques (ex: le virus *Diana*, inventé par des admirateurs de la Princesse de Galles après son décès, et qui affiche sur l'écran les deux premières lignes des paroles de "*Candle in the wind*". Il est transporté par courrier électronique(97)). En l'an 2000 le virus "*I LOVE YOU* " a pu forcer et envahir 650 sites principaux sur Internet en détruisant les fichiers *windows*;
- les dysfonctionnement du système: ralentissement, créations d'erreurs intempestives;
- l'inaccessibilité des informations: le système d'exploitation ne sait pas comment accéder aux fichiers;
- la corruption, la destruction des fichiers: le programme anéantit les fichiers en reformatant le disque dur, ou modifie les caractères au sein d'un document.

(95) "*Les virus informatiques attaquent*" Le Figaro, 22 déc. 1997; En 1996, en France près de 240 virus ont touché 6120 foyers de contaminations - "*Les virus en France statistiques 1996*" Confidentiel et Sécurité, n°33 avril 1997

(96) N. TORTELLO & P. LOINTIER, *Internet pour les juristes*, éd. Dalloz

(97) Le Monde, 23 janv 1998

- **Le ver** - C'est un programme auto reproducteur propageant des copies de lui-même au travers du réseau. Il devient une menace pour l'intégrité d'un système dés lors qu'il s'épand aux dépens du système et perturbe le réseau en le surchargeant.
- **Le bourrage de boîte (ou *spam*)** - Spécifique à Internet, cela consiste à " inonder " la boîte à lettre de la victime avec des courrier de façon à ce que la boîte ne puisse plus recevoir de courrier.
- **Le cookie**(98) sont les gâteaux empoisonnés de l'Internet. Utilisés par les fournisseurs de service, ils permettent d'identifier le type de configuration matérielle détenue par une personne connectée à l'Internet. Le *cookie* agit en fait comme un espion envoyé furtivement et collectant à l'insu de l'internaute des informations sur les sites qu'il a pu visiter, le logiciel qu'il possède et bien d'autres informations confidentielles. Leur utilisation s'est généralisée car ils sont, à l'heure actuelle, une technique de renseignement mercatique d'une exceptionnelle efficacité(99).

SECTION III: LEURS MOTIVATIONS

Il est possible d'identifier quatre facteurs principaux déterminant des individus à entrer dans le monde de la criminalité informatique: la vengeance, le besoin d'autodéfense, l'appât du gain et le défi ou la volonté d'accéder à une certaine reconnaissance sociale.

- **La vengeance**. Tel est le cas du responsable informatique qui, suite à son licenciement en 1991, plaça une bombe logique (programme de destruction à déclenchement différé) dans un programme installé sur les machines de l'employeur et causa la paralysie de l'entreprise pendant un mois(100).
- **Le besoin d'autodéfense**. Certains programmeurs utilisent ainsi des bombes logiques pour protéger leur création contre d'éventuelles contrefaçons.

(98) F. ALIN, D. LAFONT & J.F. MACARY, *Le projet Intranet*, éd. Eyrolles 1997

(99) FREDERIC-JEROME.P, La criminalité sur L'Internet, Que sais-je?, Puf, 2000, p.69.

(100) D.PADOUIN, *La criminalité informatique: le role de la police judiciaire*, Gaz.Pal, 1996, 2eme, p.1306.

L'appât du gain. Motivation criminelle universelle, les possibilités de détournement monétiques qu'offre la connaissance des réseaux informatiques sont considérables. Le détournement de numéros de cartes de crédits est ainsi devenu une activité criminelle particulièrement lucrative. En l'absence de standard sécurisé de paiement, de nombreuses enseignes de distribution proposent de valider des achats effectués via l'Internet à l'aide des données sensibles d'une carte de crédit (numéro de la carte, nom du porteur et date d'expiration). Même si la transmission de ces données est généralement sécurisée (à l'aide de modes de cryptage), les moyens de les stocker sur le serveur ne le sont pas forcément et les fichiers de numéros de cartes de crédit dans la base de données d'une entreprise peuvent être piratés.

- **Le défi ou la volonté d'obtenir une certain reconnaissance sociale** permettant de s'insérer et de se reconnaître dans un groupe.

Enfin, les motivations des *hackers* sont majoritairement dénuées d'intérêt pécuniaire et apparaissent purement idéologiques ou revendicative. Elles sont en fait dictées par la volonté d'exécuter des exploits techniques ayant pour but de valoriser certaines compétences et de démontrer la fragilité de systèmes informatiques perçus comme étant les plus fiables. Cette défiance envers les systèmes complexes n'est pas dénuée de fondement psychologique.

DEUXEME PARTIE L'ENCADREMENT JURIDIQUE DE LA CRIMINALITE INFORMATIQUE

Il est commun de reprendre l'adage selon lequel le droit pénal n'en est pas un réellement, mais constitue plutôt la sanction de tous les autres. Il est aussi courant de remarquer les limites de cette assertion. Comment dès lors prétendre élaborer un droit pénal de l'Internet, lorsque le droit pénal lui-même est contesté en tant qu'entité autonome? On l'a vu, sont protégés sur Internet des valeurs morales très différentes, de la protection de l'auteur à celle du mineur, de la manipulation des systèmes au traitement des données. A priori, il semble impossible de distinguer dans cet assemblage hétéroclite un fondement commun.

Cependant, la spécificité du droit pénal ne réside pas tant dans le fond de la protection, qui varie plus ou moins en fonction des valeurs sociales protégées par la société que dans la forme unique des sanctions qui lui sont attachées. Par conséquent, un futur et hypothétique droit pénal de l'Internet ne doit pas échouer sur l'obstacle infranchissable d'une appréhension homogène des infractions, mais se caractériser par le mode particulier d'encadrement qu'il met en place.

Cet encadrement, justement, se situe au cœur d'importantes polémiques à l'heure actuelle. L'Internet ne constitue qu'une partie infime de la réflexion plus générale et encore en chantier visant à apporter à la société la meilleure forme d'encadrement juridique possible. Deux schémas s'opposent. L'un, plus individualiste et libéral, prône une autorégulation, c'est-à-dire, une intervention minimale de l'Etat en tant qu'arbitre des conflits survenant entre les acteurs de la société, ceux-ci édictant eux-mêmes directement les normes qui leurs sont applicables[(101)]. L'autre est un composant traditionnel de la culture française, dans le sens où il réclame un Etat fort, au pouvoir d'intervention très

(101) COHEN-TANUGI (B.), " Le Droit sans l'Etat "; FUKUYAMA (F.), " La fin de l'histoire ou le dernier homme ".

large, seul capable de garantir l'intérêt général face à la multitude d'intérêts privés contradictoires.

Seulement, force est de constater que ces deux courants de pensée pris isolément échouent l'un comme l'autre dans leur mission d'encadrement sur l'Internet. La cyber-criminalité est en effet trop décentralisée pour un contrôle Etatique classique, et trop grave pour être abandonnée à un contrôle privé. Ainsi, à une insuffisance de l'autorégulation s'opposent symétriquement les limites de la régulation Etatique.

On vas aborder dans cette partie la responsabilité pénale des professionnels travaillant dans l'Internet du fait des actions des internautes **(Chapitre I)**, et les préliminairement du droit du l'Internet **(Chapitre II)**.

CHAPITRE I
LA RESPONSABILITE PENALE DES FOURNISSEURS

La nature de l'information véhiculée sur l'Internet peut engager la responsabilité civile ou pénale des acteurs de l'Internet. Mais si les services centralisés, tels que les services de communication audiovisuelle, permettent d'identifier précisément l'opérateur responsable, les services décentralisés comme l'Internet rendent délicate la détermination de la responsabilité respective des différents intervenants dans le processus informationnel, d'autant qu'un acteur peut exercer alternativement ou cumulativement plusieurs fonctions. Plusieurs actions ont été engagées ces dernières années à l'encontre des fournisseurs de l'Internet, apportant des réponses en ordre parfois dispersé.

Ce système de responsabilité, calqué sur la responsabilité éditoriale, conduit à faire peser la responsabilité sur les différents intervenant sur le réseau: auteur d' information litigieuse, fournisseur d'hébergement, fournisseur d'accès, opérateur. Ce système repose en fait sur une " présomption de surveillance " qui fait peser sur le directeur de publication la responsabilité du contrôle de la ligne éditoriale du media

concerné. Lorsqu'il est plus envisageable de faire peser sur une personne cette obligation de surveillance, le système de la responsabilité en cascade cesse.

De nombreux intervenants sont à l'œuvre dans le fonctionnement du cyberespace. Le " réseau des réseaux " naît d'une interconnexion permanente entre différents serveurs, sortes de " portails " de l'Internet. Les personnes physiques ou morales gérant ces ordinateurs seront donc prédisposés à voir leur responsabilité engagée dans le sens où ils offrent physiquement la possibilité de perpétrer le délit. Cette classe se divise en deux types de professions. Les fournisseurs d'hébergement qui prêtent de l'espace mémoire sur leurs ordinateurs pour que l'utilisateur puisse y loger un site Web; et dont la responsabilité est actuellement le sujet de vifs débats **(Section I)**. Par contre, pour l'instant et en raison de considérations techniques, le fournisseur d'accès à Internet semble moins concerné **(Section II)**.

SECTION I: LA RESPONSABILITE PENALE DU FOURNISSEUR D'HEBERGEMENT

Les fournisseurs d'hébergement stockent sur leurs serveurs les applications informatiques et les fichiers de leurs clients. Ils fournissent par ailleurs les ressources techniques et informatiques permettant aux utilisateurs d'accéder par l'Internet à ces données(102)

Distinguons deux types en pratique de fournisseur d'hébergement: d'un coté, il peut s'agir d'une entreprise dont c'est la principale occupation, offrant gratuitement ou contre rémunération de l'espace aux internautes selon la technique du contrat de louage, ses dépenses étant rentabilisés dans le premier cas par la publicité; de l'autre, la fourniture d'hébergement est un accessoire du contrat principal liant un fournisseur d'accès à ses abonnés. L'hébergement est alors plus ou moins gratuit et plus ou moins important (on compte en Méga Octets) selon la nature privée ou commerciale du site Web envisagé. Le droit, suivant la technique, n'opère pas cette distinction commerciale. Et les sources

(102) CHRISTIANE FERAL.S, *Cyber Droit*, éd. Dalloz, 1999, p.104.

textuelles permettant une mise en cause des fournisseurs d'hébergement sont multiples **(A)**, tandis que leur opportunité soulève la polémique **(B)**.

A) fondement théoriques de la responsabilité

Le fournisseur d'hébergement peut d'abord craindre qu'une adaptation systématique des textes à l'Internet ne conduise à l'application des règles dérogatoires de mise en jeu de la responsabilité en matière médiatique. Il serait alors considéré comme responsable des manquements au droit de la presse perpétrée sur son serveur, par le biais du système de la responsabilité en cascade.

Le régime de responsabilité spécifique au droit de la presse française, prévu à l'art.42 de la loi de 1881, semble en contradiction avec la culture Internet. Ce régime peut être décomposé de la façon suivante: est d'abord responsable le directeur de la publication, puis à défaut l'auteur, puis l'imprimeur, puis les vendeurs, distributeurs et afficheurs. En cas de communication audiovisuelle, le schémas est similaire: le directeur de publication, à défaut l'auteur, puis le producteur. Ce régime met en premier plan le directeur de la publication qui doit donc être en mesure de surveiller la légalité des messages diffusés, d'où l'exigence d'une fixation préalable à la communication au public.

Le fonctionnement très particulier de cette responsabilité en cascade pourrait dans l'absolu être transposé sur Internet dans cet ordre: directeur de la publication, puis auteur, puis fournisseur d'hébergement, et enfin fournisseur d'accès et même pourquoi pas, opérateur de télécommunications. Cette vision se heurte à un déficit d'acceptation par les professionnels de l'idée même d'une responsabilité du fournisseur d'hébergement.

Les conditions d'application de cette responsabilité sont-elles réunies? La jurisprudence risque de se perdre dans des discussions dont le caractère technique et contingent risque d'amener à des débats byzantins au sujet de l'exigence d'une fixation préalable. S'agit-il du transfert de l'information sur la mémoire vive du serveur, de l'utilisation de la technologie du *proxy*, de l'occupation d'espace de mémoire morte, ou faut-il à l'inverse dénier le caractère de fixation aux supports

numériques, donc par suite forcement un peu immatériels? C'est pourquoi elle a pu récemment dans un souci sans doute critiquable de répression s'écarter de cette exigence légale.

L'affaire la plus importante qui a donné lieu à l'ouverture d'une responsabilité pénale de fournisseur d'hébergement, est celle du mannequin français Estelle Hallyday qui a choisi d'engager son action à l'encontre d'un fournisseur qui hébergeait un site reproduisant dix-neuf photographies portant atteinte à l'intimité de sa vie privée. Elle demandait, sous astreinte de 100 000 francs par jour, qu'il soit fait interdiction au fournisseur de poursuivre d'une façon quelconque la diffusion des dix-neuf clichés. Le fournisseur d'hébergement s'est prévalu quant à lui de son rôle, limité selon lui, à offrir gracieusement un espace de stockage d'informations et de mécanismes de maintenance dans le cadre d'un contrat de prêt d'octets au sens des 1875 et suivants du Code Civil Français. Cet argument n'a manifestement pas convaincu le juge: "*(...) Sur la question de la responsabilité du fournisseur d'hébergement, il apparaît nécessaire de préciser que le fournisseur d'hébergement a l'obligation de veiller à la bonne moralité de ceux qu'il héberge, au respect par ceux-ci des règles déontologiques régissant le Web et au respect par eux des lois et des règlements et des droits des tiers (...); que, s'agissant de hébergement d'un service dont l'adresse est publique et qui est donc accessible à tous, le fournisseur d'hébergement a comme tout utilisateur de réseaux, la possibilité d'aller vérifier le contenu du site qu'il héberge et, en conséquence, de prendre, le cas échéant, les mesures de nature à faire cesser le trouble qui aurait pu être causé à un tiers; que pour pouvoir s'exonérer de sa responsabilité, il devra donc justifier du respect des obligations mises à sa charge, spécialement quant à l'information de l'hébergé sur l'obligation de respecter les droits de la personnalité, le droit des auteurs, des propriétaires de marques, de la réalité des vérifications qu'il aura opérées, au besoin par des sondages et des diligences qu'il aura accomplies dès la révélation d'une atteinte aux droits des tiers pour faire cesser atteinte*"(103).

(103) Ord.ref du 9 juin 1998, Estelle Lefebure / Valentin Lacambre et autres, Epertises, n°219, p.319.

Dans un arrêt du 8 décembre 1998[(104)], la chambre criminelle de la Cour de Cassation française a cassé l'arrêt relaxant un gérant de service télématique de l'infraction notamment d'apologie de crimes contre l'humanité. En l'espèce, la rubrique forum d'un service télématique intitulé " 36 15 Renouveau " et dont l'objectif était de permettre à des militants de la droite chrétienne de débattre entre eux, fut le lieu de diverses infractions de presse. Les juges du fond avaient l' relaxé, en considérant que le gérant ne possédait aucun pouvoir de contrôle sur les messages et ne pouvait être assimilé à un producteur. La Cour Suprême française par contre, visant l'art.93-3 de la loi du 29 juillet 1982, décida "*qu'ayant pris l'initiative de créer un service de communication audio-visuelle en vue d'échanger des opinions sur des thèmes définis à l'avance, Christian Ricard pouvait être poursuivi, en sa qualité de producteur, sans pouvoir opposer un défaut de surveillance des messages incriminés*".

L'espèce concerne le minitel, mais la situation est parfaitement transposable au forum que peut abriter un site Web, ou de manière générale, à l'Internet. Se référant directement à l'art.93-3 de la loi de 1982, le juge semble s'y écarter pourtant. Celui-ci dispose que: "*Au cas où une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication audiovisuelle, le directeur de la publication [...] sera poursuivi comme auteur principal lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public. A défaut, l'auteur, et à défaut de l'auteur, le producteur sera poursuivi comme auteur principal*".

Une lecture attentive montre que la condition de fixation préalable ne vise que le directeur de la publication. Seulement, la notion de producteur n'est pas définie, et il peut sembler plus juste de conditionner la responsabilité à l'exigence d'une faute ou d'un risque (la non surveillance). La fixation du message préalablement à sa communication audiovisuelle serait donc implicitement retenue en l'état actuel de la technique comme condition de la mise en jeu de la responsabilité du producteur. Les juges français, en retenant la solution contraire, font

(104) Crim. 8 déc. 1998, Bull. Crim. Déc.1998, n°335, p.973.

donc preuve de sévérité. Il est même permis de penser que la responsabilité des responsables de forums est devenue automatique, présumée irréfragablement, par un mystérieux retour aux délits matériels que le nouveau code entendait supprimer.

D'une part, ils assimilent les moyens de télécommunications à un service de communication audiovisuelle, ne cherchant pas à préciser une définition sans doute trop large. Enfin, ils refusent de distinguer entre un prestataire technique et un producteur audiovisuel. Il aurait été aussi envisageable de considérer que le gérant était une sorte de directeur de la publication, et réserver la notion de producteur à l'entreprise assurant matériellement la distribution de l'information. La solution apportée est donc critiquable puisqu'en cherchant à éviter les difficultés d'appréciation de la responsabilité du directeur de la publication, elle a artificiellement décalé le débat au niveau du producteur, terme qui n'a pas de définition sur l'Internet. A cet égard, la condition de fixation préalable posée à l'alinéa premier de l'article 93-3 fait figure d'illusion[(105)], le juge s'arrogeant le droit de modifier la qualité de la personne à loisir !

B) les moyens de limitation de la responsabilité

Face à cette responsabilité potentielle qui les menace, les fournisseurs d'hébergement réagissent de diverses manières, aux résultats plus ou moins heureux. Il est par exemple classique - il s'agit d'une clause de style - d'insérer une limitation de responsabilité dans le contrat d'hébergement. Or, il est certain que celle-ci est nulle, réputée non écrite, personne ne peut par voie contractuelle s'affranchir d'une obligation d'ordre publique. Les fournisseurs d'hébergement ont surtout tenté de faire pression sur les hommes politiques de manière à être protégés.

Fut alors votée dans la précipitation la loi FILLON du 18 juin 1996 qui voulait modifier les art.43-2 et 43-3 de la loi de 1986 dans ces termes: "*ne sont pas pénalement responsables des infractions résultant du contenu des messages diffusés par un service de communication audiovisuelle si ce*

(105) LASSALLE (J. Y.), note sous l'arrêt du 8 décembre 1998, JCP 1999, à paraître.

service n'a pas fait l'objet d'un avis défavorable publié au Journal Officiel, sauf s'il est établi qu'(ils) ont, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission". Ces articles ont été déclarés inconstitutionnels(106). Il faut en effet confronter cette tentative avec la jurisprudence antérieure du conseil constitutionnel: "*Considérant que nul ne saurait, par une disposition générale de la loi, être exonéré de toute responsabilité personnelle quelle que soit la nature ou la gravité de l'acte qui lui est imputé*"(107). De manière paradoxale et inattendue, les positions des juges américains et français se rejoignent ici, la " Decency Act ", loi dont l'objectif était de limiter la responsabilité des professionnels d'Internet, a été déclarée inconstitutionnelle par certaines cours, selon l'idée qu'une liberté d'expression absolue doit avoir pour corollaire une responsabilité très large.

L'idée d'une réforme législative n'en est pas pour autant enterrée, et semble même faire l'objet d'un curieux consensus politique(108). Par exemple, le député socialiste français Patrick BLOCHE a déposé le 18 mai 1999 un amendement au projet de loi sur l'audiovisuel dans ce sens. "*Je veux appliquer la responsabilité de l'hébergeur à deux conditions: s'il a lui-même participé à la création du contenu illicite, ou si ayant été saisi par une autorité judiciaire, il n'a pas empêché l'accès à ce même contenu.*"(109). La tendance actuelle serait donc de ne pas abandonner un pouvoir de censure à l'hébergeur, celui-ci devant attendre une décision judiciaire. Mais la procédure semble un peu absurde: un premier référé serait nécessaire pour faire constater à l'hébergeur le contenu des sites qu'il propose, et, s'il n'agit pas, un second référé deviendrait obligatoire pour mettre en jeu sa responsabilité. Le texte adopté en première lecture par l'assemblée nationale écarte donc en pratique totalement la responsabilité de l'hébergeur, puisque dans tous les cas une action débouche sur une demande de suppression des données litigieuses, et il suffit au

(106) Décis. n°96-378 DC, Cons. Constit. 23 juillet 1996, JO 27 juillet 1996, p.11400.

(107) Décis. n°88-248 DC, Cons. Constit. 17 janvier 1988.

(108) "Madelin, Strauss-Kahn: même combat ", Expertises avril 1999, p.85.

(109) LENGLART. E, *L'hébergeur et les amendements*, Le Monde, supplément nouvelles technologies du 19 mai 1999, accessible sur Internet.

professionnel pour être exonéré d'attendre que le juge intervienne; la victime ne pourra pas arguer de son comportement antérieur valant approbation implicite. Cette procédure n'est aussi applicable qu'en cas de délit continu, ce qui n'est pas le cas de tous les types de criminalité intervenant sur Internet.

Le fond de la réforme semble s'inscrire dans un consensus: on ne peut incriminer un hébergeur pour le contenu de ces sites, à moins qu'il soit tel qu'il est présumé en avoir connaissance. Ce consensus n'est qu'apparent, car, le problème réel, la possibilité ou non pour le professionnel de contrôler les sites qu'il héberge est ignorée. Les extrêmes sont envisageables: soit on décide que l'hébergeur a une obligation très forte de contrôle, (et par anticipation, les fournisseurs forment déjà des groupes de surveillance interne), soit, sous le prétexte de l'instantanéité de l'information, on admet que l'hébergeur attende que des réactions se manifestent pour vérifier la licité du site hébergé.

Le dernier type de défense est alors par nature judiciaire. La jurisprudence, si elle semble de manière générale défavorable aux fournisseurs d'hébergement, ne leur accorde pas moins quelques victoires. Il a été ainsi jugé que la disparition de l'adresse DNS du site contraire à l'ordre public le jour de l'audience permettait à hébergeur d'être provisoirement exonéré. Le juge refuse en effet de statuer en référé, considérant qu'il n'y avait plus de troubles à l'ordre public(110). Seulement, en l'espèce il ne s'agissait pas d'une disparition mais d'un simple déménagement technique de l'adresse. Cette décision peut sembler critiquable quand on sait d'une part l'importance du référé dans les litiges concernant Internet, et d'autre part, la facilité de déménagement d'un site sur la toile. Est donc de nouveau posé le problème de la création d'un référé Internet spécifique.

SECTION II: LA RESPONSABILITE PENALE DU FOURNISSEUR D'ACCES

Les fournisseurs d'accès à l'Internet offrent à leurs clients les ressources techniques permettant aux utilisateurs d'accéder aux services.

(110) CA Paris, 10 février 1999, V. Lacambe c/ E. Hallyday, LP avril 1999, n°160, III, p.52.

Ils permettent d'établir la connexion entre les fournisseurs de services et les utilisateurs qui se connectent à l'Internet, au besoin par l'intermédiaire de leurs propres fournisseurs d'accès[111].

Nous allons traiter la première décision en France concernant la responsabilité, il s'agit de l'affaire UEJF **(A)**, et est ce qu'il y a possibilité de mise en jeu cet responsabilité? **(B)**.

A) L'affaire UEJF de 1996

La notion de responsabilité des fournisseurs d'accès n'est pas encore résolue, même si paradoxalement, elle fut l'objet en France d'une des premières décisions concernant l'Internet. Il s'agit de l'affaire UEJF (Union des Etudiants Juifs de France). En l'espèce, cette association, scandalisée par la diffusion de sites Web au contenus négationnistes, attaqua en justice le 15 mars 1996 la majorité des principaux fournisseurs d'accès français (en anglais, " provider "): *Calvacom, Eunet, Axone, Oléane, Compuserve*[112]*, Francenet, Internetway, GIP Renater, Imaginet*. Leur objectif était d'obtenir du juge l'interdiction de la diffusion des messages par les défenseurs.

Leur but était sans doute trop flou, mais permettait de confronter tous les aspects du problème. D'un coté, il est certain que les fournisseurs d'accès sont directement responsables (au sens large) de la lecture des messages, puisque c'est la réunion de leurs serveurs qui constitue à proprement parler, le net francophone. Seulement, est-il techniquement possible d'interdire l'accès à un site? Il est envisageable en théorie de créer une liste noire sur laquelle serait inscrites toutes les adresses IP interdites et de refuser les demandes d'accès à celles-ci. Mais cela obligerait à un changement de toute la structure, des modalités de fonctionnement, étant donné qu' Internet, par son coté décentralisé, limite les possibilités de

(111) CHRISTIANE FERAL.S, *Cyber Droit*, éd. Dalloz, 1999, p.107.

(112) On rappellera cependant qu'en Allemagne, la responsabilité du fournisseur d'accès *Compuserve* a été mis en cause le 28 mai 1998 par un tribunal de Munich, Celui-ci été contraint de fermer l'accès à des forums pornographiques dont les images et textes enfreignaient les articles du Code pénal allemand réprimant la diffusion de certains formes de pornographie (pédophilie, zoophilie, sadomasochisme)

censure. Comprenant par la suite les difficultés auxquelles ils s'exposent, les membres de l'UEJF changèrent par la suite d'objectif, et réclamèrent une charte de la part de certains fournisseurs d'accès. En tout cas, leur demande, trop imprécise, fut rejetée(113).

Leur action ne s'est pas soldée par un échec total. D'une part, ils ont obtenu des fournisseurs qu'ils pratiqueraient un certain contrôle. Ensuite, cette affaire a été l'objet d'une prise de conscience par les juristes de leur dépendance à l'égard de la technique en ce domaine, et a été évité l'ébauche d'un procès de l'Internet. Les fournisseurs d'accès y ont pour la première fois développé la théorie dite " du tuyau ", expliquant qu'ils n'étaient que de simples intermédiaires techniques fournissant la liaison à Internet, tel un tuyau. Cette image est significative des moyens dont dispose le fournisseur: soit il coupe l'accès, soit il laisse le contenu se déverser sans avoir la possibilité matérielle de trier selon sa légalité ou non.

B) La possibilité réelle de mise en jeu de la responsabilité du fournisseur d'accès

En définitive, il apparaît que la responsabilité du fournisseur ne peut en théorie pas être engagée pour les délits de presse commis par un de ces abonnés sur le Web, le fournisseur d'hébergement étant avant lui responsable. Cela ne clos pas tout débat. Notamment, il reste le problème des services de forums. S'il est impossible par avance de connaître quel site un individu va consulter, on peut par contre supposer le contenu de messages postés dans des forums tels que " alt.sex.pedohilie " par exemple ! Cela a conduit en Allemagne un juge à interdire aux fournisseurs d'accès toute diffusion de 200 de ces forums(114). Seulement, et on touche là encore à la fois aux contingences techniques qui limitent l'application de la règle de droit et à l'interdépendance de chaque pas dans la lutte contre la cyber-criminalité, le fournisseurs d'accès a été forcé en même temps de supprimer l'accès sur toute la planète de ceux-ci, son logiciel ne permettant pas à l'époque de distinguer les abonnés allemand des autres. Dans une autre affaire en Allemagne, le ministère public imposa aux fournisseurs d'accès de

(113) TGI Paris, 12 juin 1996, DIT 1997/2, p. 36.

(114) Affaire *Compuserve*. Condamnation de son ancien dirigeant, Felix SOMM, à deux de prison avec sursis par le tribunal de Munich, Libération 5 juin 1998, supplément multimédia.

bloquer l'accès à un site délictueux néerlandais. Cependant, cela bloqua l'accès à tout le serveur, notamment les pages légales, et autre effet indésirable, par réaction, les internautes ont multiplié les sites miroirs reprenant la page Web censurée. Ces deux affaires au succès différent montrent qu'un contrôle a priori du Web par le biais des fournisseurs d'accès est irréalisable. Toute responsabilité de ceux-ci ne peut être qu'a posteriori. Cela laisse donc une marge de manœuvre au professionnel, donc en d'autres termes, une possibilité de corégulation.

Les fournisseurs d'accès ne sont pas exonérés de toute responsabilité pour autant, comme ils se plaisent eux-mêmes à le remarquer: "*La responsabilité de droit commun, applicable aux acteurs professionnels ou particuliers, au cas par cas, jointe à une politique d'autorégulation, de filtrage et de formation s'inscrivant notamment dans le plan d'action communautaire, permet de protéger les utilisateurs*"(115). Un fournisseur d'accès n'assurant pas une protection suffisante de l'enceinte de son serveur pourrait ainsi être condamné par application de l'art.226-17 C.P.F qui réprime le traitement automatisé de données nominatives sans protection, à supposer établies les conditions d'application générales à la notion de donnée personnelle. La responsabilité principale qui pourrait leur incomber repose sur la notion de risque, largement admise en droit civil, mais assortie de conditions très restrictives en droit pénal. Par exemple, un fournisseur qui ne met pas en place un robot de filtrage sophistiqué(116) des messages envoyés sur un forum est quelque part responsable de la publication, le cas échéant, de ceux-ci. Mais il n'y a pas au sens pénal mise en danger de la vie d'autrui ! Sur ce plan, donc, le fournisseur ne devrait pas encourir de sanctions pénales.

CHAPITRE II
LES DEBUT DU DROIT DE L'INTERNET

Depuis quelques années, les juridictions prennent conscience que l'Internet implique une nouvelle forme de délinquance et fait apparaître

(115) AFA, "*préconisation sur la réglementation applicable à Internet*", sur le web.

(116) Petit logiciel reconnaissant automatiquement les messages à écarter, en reconnaissant l'adresse IP de son destinataire ou en présumant le contenu du message du nombre d'expression immorales employées.

sous de nouvelles formes des infractions fort anciennes. Les juridictions commencent timidement à s'intéresser aux infractions liées à Internet et découvrent peu à peu que l' arsenal juridique est tout à fait apte à s'appliquer à la " cyber- délinquance ". Toutefois, la majorité des décisions ne relèvent que de tribunaux de grande instance ou de tribunaux de commerce, statuant en référé. Cela permet cependant de remarquer que les juridictions se sont intéressées en priorité à certaines infractions.

Nous allons étudier les difficultés qu'ils ont rencontrées en mettant en œuvre la répression **(Section I)**, puis les améliorations du droit du l'Internet **(Section II.)**.

SECTION I: LES DIFFICULTES

Nous avons vu que les juridictions se montraient prudentes dans leur attitude face aux comportements répréhensibles constatés sur Internet. Cela s'explique par les grandes difficultés, tant juridiques **(A)** que techniques **(B)**, qu'elles rencontrent en la matière.

A) Les difficultés juridique

Ces difficultés résultent notamment du caractère international du réseau **(1)** et de la multiplicité des acteurs qui y interviennent **(2)**.

1) L'application de la loi pénale dans l'espace

La détermination de la loi pénale applicable aux comportements précédemment décrits constitue une difficulté importante du fait de l'absence de frontières sur Internet. Certaines solutions, adaptées à sa spécificité semblent toutefois envisageables.

Internet est un réseau mondial qui permet de communiquer sans distinction de frontière. Cela procure beaucoup d'avantages au point de vue de l'échange, mais crée également des situations extrêmement complexes.

On peut imaginer que sur un *NewsGroup* hébergé par un serveur allemand, un pédophile anglais diffuse des images pornographiques d'enfants, images qui pourront être vues par un français ou un américain.

Il se peut également qu'un serveur japonais mette en place une escroquerie dont les victimes seraient de toute nationalité. Pour en finir avec les exemples, un français peut s'introduire sur le site public de la CIA ou dans un réseau interne d'une grande entreprise américaine pour y ajouter des données.

La question se complique nettement lorsque de plus le comportement en question est pénalement sanctionné dans certains pays mais pas dans d'autres. De nombreux sites révisionnistes ont été créés aux Etats-Unis(117), où ce type de messages ne fait l'objet d'aucune interdiction, en vertu aux Etats-Unis du Premier Amendement de la Constitution qui garantie un droit d'expression quasi-illimité. Or ces sites sont consultables en France. A l'inverse, certaines interdictions pénalement sanctionnées sont prévues par des législations étrangères, sans l'être par la loi française. Ainsi, le droit coranique interdit toute représentation du Prophète sous peine de sanctions religieuses et pénales.

La règle générale veut que le crime commis par le biais de l'Internet soit un crime temporaire où l'activité criminelle a lieu dans un seul et même endroit. Ainsi se pose la question de savoir quelle loi appliquer dans ce cas de crimes?

Examinons à titre d'exemple, le cas où un individu commet un acte nécessitant l'application à son encontre d'une certaine peine. Si cet acte a lieu au Koweït, la loi appliquée sera la loi pénale Koweïtienne, et cela en application de l'article 1 traitant de la territorialité des lois, et stipulant que: "*Les articles de cette loi sont applicables à l'encontre de tout individu commettant un crime sur le territoire koweïtien*".

Cependant, dans l'éventualité où un ressortissant Français, résidant aux Etats Unis d'Amérique, insulte un ressortissant Indien résidant aux Pays-Bas en usant du courrier électronique et envoie des copies de ce courrier à d'autres individus résidant au Japon, au Koweït et en Egypte. Dans ce cas de figure, quelle loi territoriale, doit- on appliquer?

(117) ainsi qu'aux Pays-Bas

Nous voyons ici que la loi Koweïtienne doit-être appliquée étant donné qu'une partie du crime a eu lieu sur le territoire Koweïtien, et cela selon le même article pré-cité, stipulant que: "*Est puni tout individu ayant commis en dehors du territoire Koweïtien un acte le rendant l'auteur original ou simplement partenaire dans une action incriminée par la loi Koweïtienne et dont tout ou partie a lieu sur le territoire national*."

De ce fait, cet acte sera jugé par les cours Koweïtienne et par la même par toute autre cour de tout autre pays où partie de ce crime aurait été commis.

Dans le cas où l'acte criminel par le biais de l'Internet aurait été entièrement commis en dehors du territoire national, seront applicables les lois *nationales et cela en* application de l'article 12 de la même loi disant en la personnalité de la loi pénale.

Aussi, les règles de la loi Koweïtienne seront applicables selon le principe de la personnalité positive, si un ressortissant Koweïtien commet par le biais de l'Internet un acte incriminé sur un autre territoire puis retourne au Koweït(118).

En France, les mêmes lois sont applicables dans les cas de crimes ou de parties de crimes commis par le biais de l 'Internet, sur le territoire Français(119) (Art. 3/112).

2) La "Nétiquette"

Les internautes se sont spontanément engagés à respecter certaines règles, qui sont désormais contenues dans ce qu'on appelle la Nétiquette: cette dernière "*est valable et admise internationalement, car elle n'a été imposée par personne en particulier, elle s'est imposée presque naturellement à tous*"(120). Celle-ci se présente sous la forme de dix commandements(121):

- Tu n'emploieras pas l'ordinateur pour nuire à autrui;

(118) Art.12 du C.P.K

(119) Art. 3/112 du C.P.F

(120) "Pour une intégration sereine et un développement harmonieux d'Internet dans la société française " Rapport de l'Association des Utilisateurs d'Internet du 7 juin 1996 - **http://www.aui.fr/Rapports/RAUI-070696.html**

(121) en provenance du Computer Ethics Institute - **http://www.fau.edu/rinaldi.net**

- Tu ne brouilleras pas le travail informatique d'autrui;
- Tu ne fouineras pas dans les fichiers des autres;
- Tu n'emploieras pas l'ordinateur pour voler;
- Tu n'emploieras pas l'ordinateur pour faire de faux témoignages;
- Tu n'emploieras, ni ne copieras du logiciel que tu n'as pas payé;
- Tu n'emploieras pas les ressources informatiques d'autrui sans autorisation;
- Tu ne t'approprieras pas le travail intellectuel d'autrui;
- Tu songeras aux conséquences sociales du programme que tu écris;
- Tu emploieras l'ordinateur de manière à faire preuve de considération et respect;

Chaque service d'Internet dispose de règles d'usage encore plus précises. Celui qui ne les respecterait pas s'expose à la vengeance des autres internautes, soit par des *flames* (messages injurieux) soit par le blocage de son courrier ou de son site.

Pour certains internautes, le droit n'a pas à appréhender les comportements qui s'expriment sur le réseau et ils ne reconnaissent tout au plus que " l'autorité " de la Nétiquette. Il faut rappeler qu'Internet a été conçu par et pour les universitaires comme un espace de liberté sur lequel l'information devait pouvoir être communiquée et échangée sans limitation. Les internautes américains se fondent parfois sur le Premier Amendement de leur Constitution qui leur garantie la liberté d'expression. Ces derniers ont d'ailleurs remporté une victoire en juin 1997 en obtenant de la Cour Suprême la déclaration de l'inconstitutionnalité du *Communications Decency Act* (CDA), qui interdisait "*l'utilisation d'un service interactif en ligne pour diffuser à l'intention de mineurs des obscénités ou des propos indécents constituant une atteinte évidente aux normes de la société contemporaine*"[(122)].

(122) Cour Suprême des Etats-Unis 26 juin 1997 Reno V. ACLU - **http://www.aclu.org - http://epic.org** " Au fil du Net " Gaz. Pal. 10, 12 août 1997 - La cour confirme les décisions d'août 1996 des tribunaux de Philadelphie et de New York qui considéraient que cette loi limitait de façon abusive le droit des citoyens adultes d'échanger des propos et des informations. Le Sénat a cependant voté une nouvelle proposition de loi visant les sites web commerciaux affichant des =

Mais cette liberté doit tout de même être limitée dans la mesure où des intérêts plus importants sont en jeu, comme ceux que protègent le droit pénal(123). De plus, ce n'est pas parce que le réseau est une nouvelle technologie et une nouvelle forme de communication qu'il doit échapper au droit. Celui-ci a vocation à s'appliquer à tous les domaines que l'être humain appréhende(124). A fortiori dans certaines hypothèses où les atteintes sont graves. Comme l'exprime l'Association des Utilisateurs d'Internet: "*Lorsqu'il ne s'agit plus de comportements problématiques, mais de comportements réellement délictueux, la "Nétiquette" est clairement dépassée, et lorsque le délit est constitué, c'est la loi qui doit s'appliquer afin d'identifier les responsables, d'établir leur culpabilité, de les sanctionner, et de faire cesser, dans la mesure du possible, l'objet du délit*". En effet, la " Nétiquette " constitue certainement un engagement de bonne conduite sincère des internautes, mais elle n'a aucun caractère contraignant. Tout au plus un arbitrage peut-il se fonder sur ses règles (on parle parfois de *Lex Cybernautica*(125)) mais pas le prononcé de sanctions de nature pénale.

documents " nuisibles pour les mineurs ",ainsi qu'une proposition visant à obliger les écoles et bibliothèques recevant des subventions fédérales à mettre en place des systèmes de filtrage de sites " inconvenants " (ces projets doivent être examinés par la Chambre des Représentants): "*Le cyber-sexe à nouveau dans la ligne de mire*" Le Monde Cahiers multimédia 23, 24 nov. 1997 - "*Vers un CDA Bis*" Le Monde 9 sept 1998

(123) N. BRAULT cite dans "*Le droit applicable à Internet*" **(http://www.grolier.fr/cyberlex.net)** le juge américain S. Dalzell (dans l'aff. ACLU vs Reno - Trib. Fédéral de Philadelphie 11 juin 1996): "*La pédophilie et l'obscénité n'ont aucune protection constitutionnelle, et le Gouvernement peut les bannir de certains médias, ou de tous. La liberté d'expression à laquelle se réfère le premier amendement ne comporte pas la liberté d'ignorer les limitations traditionnelles*". Un journaliste américain, enquêtant sur la pédophilie sur Internet, fait d'ailleurs l'objet de poursuites pour détention et trafic d'images pédophiles devant un tribunal du Maryland qui lui a refusé le droit d'invoquer le 1er amendement: Le Monde, 10 juill. 1998, **http://www.legalis.net**

(124) C'est ce que reconnaît la charte Safety-Net qui a été créée en Grande-Bretagne pour lutter contre la pédophilie: "*The Internet is not a Legal Vacuum: In general, the law applies to activities on the Internet as it does to activity not on the Internet. If something is illegal "off-line" it will also be illegal "on-line", and vice versa.*"

(125) " Libres propos pour une " Lex Cybernautica " " J.C. Galloux dans "*Expertises pour l'an 2000*" éd. Des Parques

B) Les difficultés techniques

Les difficultés techniques sont liées aux méthodes de cryptologie employées sur le réseau (1) et à la difficulté de se procurer la preuve des infractions commises via Internet (2).

1) Cryptologie

Les difficultés techniques sont surtout afférentes à la question de la cryptologie. Cette dernière "*permet de verrouiller des données à l'aide d'un mot de passe ou d'un système intégré de façon à empêcher un tiers non autorisé d'avoir accès aux données ou de les reproduire*"(126).

Les logiciels de cryptage assurent la protection de trois fonctions:

- **L'intégrité:** ils permettent de détecter toute altération, modification, ajout, réutilisation de l'information
- **La confidentialité:** il ne peut être lu que par son destinataire
- **L'authentification:** son utilisateur peut identifier l'émetteur ou un utilisateur du système, ce qui permet une véritable " signature électronique ". De plus, cela évite toute " non-répudiation ", c'est à dire qu'un émetteur nie avoir envoyé un message.

Grâce aux logiciels de cryptage, les individus peuvent coder les informations qu'ils s'échangent et ainsi en assurer la confidentialité. Cette donnée est essentielle pour le développement du commerce électronique car on imagine mal que les gens accepteront de laisser sur le Net leur numéro de carte de crédit ou d'acquérir un porte-monnaie virtuel s'ils peuvent être utilisés par le premier venu après avoir " volé " l'information.

Le revers de cette médaille est que la cryptologie peut également servir à des communications moins innocentes, telles celles de terroriste, de nazis, de mafiosi, de trafiquants de toute sorte(127). D'où la nécessité de le réglementer, selon la France, pour en limiter l'utilisation. Mais dès

(126) P. NICOLEAU, "*La protection des données sur les autoroutes de l'information*", D. 1996 chron. P.111

(127) S. LE DORAN & P. ROSE, Cyber mafias, éd. Denoël 1998, p.120: la cryptologie aurait été utilisée dan 500 affaires criminelles jusqu'à présent et devrait être utilisée en 2001 dans 16000 affaires.

lors qu'on l'autorise, se pose la difficulté de pouvoir décoder quand on en aura besoin certains messages.

Le terme le plus exacte serait plutôt celui de " cryptographie ", reconnu par le dictionnaire et qui vient des mots grecs " cacher " et " écrire ", mais la pratique parle de cryptage ou de cryptologie sans vraiment différencier leur sens. Quoiqu'il en soit, cette technique permet de coder et de décoder un message, dès lors que l'on a connaissance du mécanisme de chiffrement.

L'algorithme est ce procédé qui permet de passer d'un message clair à un message codé et inversement. Il repose sur une clé contenant un certain nombre de caractères: Plus y a de caractères, plus le code est difficile à découvrir. Il permet de coder le message soit en substituant les éléments du message à d'autres caractères, soit en modifiant l'emplacement de ces éléments dans le message.

On distingue deux types de chiffrement:

- **Le chiffrement symétrique:** La même clé est utilisée pour chiffrer et déchiffrer le message, d'où la nécessité que cette clé demeure secrète. Elle ne doit être connue que des personnes qui veulent communiquer entre elles par ce moyen.
- **Le chiffrement asymétrique:** Dans cette hypothèse, chaque individu possède deux clés. Il communiquera la première d'entre elles, que l'on appelle clé publique, aux autres personnes (par exemple sur sa carte de visite) et ces dernières pourront lui écrire en l'utilisant. Seul le destinataire, qui aura la seconde clé, la clé privée, pourra lire ce message.

2) les preuves

Ce qui caractérise les crimes commis par le biais de l'Internet est le fait qu'ils soient difficiles à découvrir.

Et même dans les cas où de tels crimes sont découverts, la poursuite des auteurs reste très difficile étant donné que les preuves classiques ne conviennent pas à de telles fins vu que les autorités se heurtent à les techniques informatiques très développées dont se servent les criminels de

l 'Internet pour masquer leurs crimes et anéantir toute trace de preuve possible.

De plus, la majorité des procédures pénales ne sont ni suffisantes ni adéquates pour les fins d'investigation et de jugement dans ce cadre de crimes.

Il en découle qu'il est urgent de trouver des procédures pouvant se plier aux exigences nouvelles imposées par la technologie.

Regardons dans ce cadre de plus près les législations des Etats Unis et de la France:

- **Aux Etats unis d'Amériques:** La jurisprudence a discuté des problèmes pratiques naissant des crimes commis par le biais de l'Internet et des procédures pénales adéquates notamment en ce qui concerne l'ordre du juge de perquisitionner et la nécessité que ce dernier ait de bonnes notions dans le domaine de l'informatique sinon sa décision peut devenir nulle. De plus, quand le juge donne son ordre de perquisition, il doit le faire avec beaucoup de précision et d'attention aux détails, ne laissant rien ainsi à l'estimation de l'agent exécutant cette perquisition. 'ordre de perquisition ne peut en aucun cas être d'ordre général selon la première modification de la loi Américaine qui prévoit que quand la perquisition a pour objet des affaires en relation avec l'expression d'opinion, ces dernières doivent être minutieusement décrites et émanant de preuves solides et non de simples doutes des autorités.
- **En France:** La situation en France est similaire à celle aux Etats Unis d'Amériques en ce qui concerne les procédures pénales dans le cadre des crimes de l'Internet et où rien ne s'oppose à l'application des règles générales des procédures pénales, en observant la nécessité que la perquisition ne soit pas d'ordre général, afin que la vie privée du prévenu soit préservée. Dans ce contexte, il est important de mentionner que le législateur français prête une attention particulière à ce qu'il n'y ait pas atteinte à la vie privée des individus. Ainsi l'article 9 du droit civil a protégé la vie privée en incriminant les actes qui peuvent lui nuire tel que le fait de photographier un individu, d'enregistrer sa voix ou de lire ses correspondances sans son autorisation. (C.P.F 2/15-226). Cet article couvre sans doute les

courriers électroniques selon le principe de communication stipulé dans la loi du 1986.

SECTION II:
LES AMELIORATIONS DU DROIT DE L'INTERNET

Il est certain que certaines dérives sont apparues sur Internet et que le droit est peut-être insuffisant pour les contenir. La solution viendra sans doute d'une prise de conscience du phénomène Internet et d'une adaptation à sa typologie. Mais compte tenu justement de ses spécificités, il est également nécessaire d'allier au droit les initiatives des utilisateurs de l'Internet.

Nous allons traiter deux efforts, les efforts des Etats **(A)**, et les efforts des acteurs **(B)**

A) Les efforts des Etats

Les Etats se doivent d'agir, de façon collective **(1)** et individuelle **(2)**.

1) Les efforts collectifs

Dans le cadre de l'Union européenne, une directive relative aux services en ligne pourrait voir le jour. L'Union a écarté du champ d'application de la directive Télévisions sans frontières les services Internet, visiblement car la question était trop complexe. Mais nous pourrions nous inspirer de cette directive pour réglementer ces services ainsi que les services de télévision point à point. Comme pour la directive du 3 octobre 1989 modifiée le 30 juin 1997, le principe de l'application du droit du pays émetteur pourrait être retenu entre les Etats membre, sauf atteinte grave à l'ordre public de l'Etat récepteur, et l'application du droit du pays de réception lorsque l'émission provient d'un Etat non-membre.

On peut se féliciter que des initiatives voient le jour. En matière de protection des droits d'auteur et de droits voisins, la France a ratifié en octobre 1997 dans le cadre de l'Organisation mondiale de la propriété industrielle (OMPI) deux accords élargissant la protection de ces droits. Dans le courant de l'année 1998, la négociation de l'adoption de la directive " sur le droit d'auteur et les droits voisins dans la société de

l'information"[128] aura lieu[129]. Rappelons qu'une directive visant la protection des bases de donnée a déjà été adoptée.

L'Union européenne s'inquiète également de la présence sur Internet de sites à contenu illégal et préjudiciable car elle peut "*sérieusement entraver le développement de l'industrie Internet émergente et ainsi, affecter la mise en place du nécessaire environnement favorable propre à permettre aux initiatives et entreprises de s'épanouir*"[130]. Ce problème a ainsi donné lieu à un certain nombre de communications, résolutions et livres verts relatifs au contenu illégal et préjudiciable sur le réseau Internet[131]. La Commission considère qu'il est "*indispensable d'arrêter une législation commune qui prohibe explicitement l'utilisation d'Internet*" pour la diffusion de messages condamnables[132]. Elle ajoute que des dispositions doivent être prises pour limiter la vente de médicaments sur Internet à ceux qui ne nécessite ni prescription, ni surveillance médicale et que doit être élaborée une politique commune sur la traite des êtres humains.

En ce qui concerne l'application de la loi pénale et la responsabilité des acteurs, elle "*invite instamment les autorités nationales compétentes à coopérer afin de parvenir à un accord international définissant les contenus illégaux et, par conséquent, passibles de sanctions quelque soit le lieu de résidence du fournisseur de contenu*" et "*propose l'établissement de catalogues "nationaux" aisément accessibles, recensant les contenus ou les opérations illégales détectées sur Internet*". De plus, la Commission "*souligne que la responsabilité des fournisseurs d'accès et de services devrait être réglementée aux échelons communautaire et international*".

(128) adoptée par la Commission européenne le 10 déc. 1997

(129) " Préparer l'entrée de la France dans la société de l'information" **http://www.culture.fr/**

(130) proposition de décision du Conseil faite par la Commission 26 nov 1997 - COM(97) 582 final cons.2

(131) Livre vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels du 6 oct. 1996 (COM(96) 483final), communication de la commission sur le contenu illégal et préjudiciable sur le réseau Internet du 16 oct. 1996 (COM(96) 487 final), Résolution du Conseil relative au contenu illégal et préjudiciable sur Internet du 17 févr. 1997 (JO n°C70,6.3.1997,p.1), résolution du Parlement européen relative au contenu illégal et préjudiciable sur Internet du 24 avril 1997 **http://europa.eu.int**

(132) racisme, incitation à la haine ou à la violence, terrorisme, pornographie déviante, négationnisme, exploitation des enfants pour une activité sexuelle selon la Commission

Pour mettre en œuvre cette politique, la Commission a proposé une décision du Conseil relative à un " plan d'action visant à promouvoir une utilisation sûre d'Internet "[133]. Ses principaux axes sont de:

- créer un environnement sûr en créant des lignes directes (ou *hot-lines*) sur les quels les internautes pourraient signaler les sites qui leur semblent véhiculer des contenus illégaux, ainsi qu'en encourageant les initiatives d'élaboration de code de bonne conduite;
- développer et unifier les systèmes de filtrage et de classification des contenus des sites;
- sensibiliser les individus aux excès qu'Internet peut présenter.

La Commission insiste de plus en plus sur la nécessité d'une coordination internationale qui pourrait se matérialiser par une "Charte internationale "[134].

De plus, un comité d'experts sur la criminalité dans le cyberespace ("PC-CY") a été établi au sein du Conseil de l'Europe. Ce comité doit établir un instrument juridique contraignant pour combattre notamment les infractions graves commises lors de l'utilisation d'Internet[135].

Il est important que face à une délinquance internationale, les Etats s'entraident. Il existe de nombreux accords relatifs à la coopération judiciaire et policière (extradition, exequatur), encore faut-il les appliquer et peut-être aussi simplifier les procédures. Ainsi, les procédures d'exécution des commissions rogatoires internationales pourraient peut-être être allégées.

Il serait temps de mettre en mouvement les dispositions de la Recommandation du Conseil de l'Europe 95 R 13 relative aux problèmes de procédure pénale liés à la technologie de l'information, et notamment

(133) Communication de la Commission du 26 nov 1997: " Plan d'action visant à promouvoir une utilisation sûre d'Internet " COM(97) 582 final

(134) la commission la définit comme " un accord multilatéral sur une méthode de coordination ". Communication de la Commission du 4 février 1998 " La nécessité de renforcer la coordination internationale " COM(98) 50 final

(135) "*Contenu illégal et préjudiciable sur Internet*" rapport intermédiaire 4 juin 1997 **http://europa.eu.int**

les art. 17 et 18 de son annexe, qui favorisent les perquisitions internationales.

La réunion des ministres de l'Intérieur et de la Justice du G8 à Washington le 10 décembre 1997[136] a peut-être mis en marche ce mouvement de coopération. Chacun des pays s'est engagé à créer un " point de contact " disponible 24h/24 pour suivre les affaires transnationales, s'assurer que des personnels spécialisés en nombre suffisant soient disponibles, réexaminer son arsenal juridique, établir des procédures afin de permettre la conservation des preuves et les perquisitions en matière informatique.

Les Etats-Unis avaient même proposé la création d'un Bureau international de la criminalité informatique.

Or, cette coopération va s'avérer difficile par le fait que chaque Etat a une attitude différente à l'égard du réseau.

2) Les efforts individuels

Alors que certains Etats laissent à Internet la possibilité de " s'épanouir " en toute liberté comme les Pays-Bas[137], d'autres Etats ont fait le choix de réglementer l'accès à Internet. La Thaïlande a mis au point un projet de loi visant à établir une censure très stricte et un contrôle étatique complet sur le contenu et les infrastructures d'Internet dans le pays[138].

La Chine à pris quant à elle de nouvelles dispositions pénales visant à s'appliquer aux infractions commises sur Internet et punies de " sanctions criminelles "[139]. Singapour a étendu les dispositions relatives à la censure des documents à caractère sexuel et a aggravé les peines[140].

(136) "*Les ministres du G8 adoptent un plan d'action contre la criminalité informatique*" Le Monde 12 déc. 1997

(137) "*Internet, l'Europe et la censure*" Le Monde, Cahiers multimédia 23, 24 fevr. 1997

(138) Le Monde, 8 janv 1998

(139) Le Monde, 6 janv. 1998

B) Les efforts des acteurs

Nous ne devons pas oublier qu'Internet est à l'origine un réseau sur lequel règne la plus grande liberté. Les internautes n'apprécient guère les intrusions des Etats et leur volonté de le contrôler. En laissant les utilisateurs s'auto-réguler, nous obtiendront sans doute de meilleurs résultats. Préférer l'autocontrôle au contrôle à priori est d'ailleurs la première proposition du Rapport FALQUE-PIERROTIN(141).

Dans ce qui suit nous traiterons du rôle de certains acteurs **(1)**, et l'auto-réglementation **(2)**.

1) Le rôle de certains acteurs

Les rôles se doivent d'agir, de façon contre la fraude informatique **(a)** et contre les contenus préjudiciables **(b)**.

a) Contre la fraude informatique(142)

Le meilleur moyen de se prémunir contre les fraudes est encore de ne pas se connecter au réseau. C'est pourquoi par exemple, le Ministère de la Défense Française(143) a prévu que "*les stations et terminaux doivent être dédiés exclusivement à l'utilisation d'Internet et ne mettre en œuvre aucune autre application*".

Mais ce choix n'est pas toujours possible. Il faut alors se doter de moyens de prévention à l'encontre des pirates. La loi impose même parfois à certains organismes de protéger les données qu'ils détiennent(144). Malheureusement, ces moyens sont insuffisants comme nous allons le voir (d'autant plus qu'il faut les mettre à jour régulièrement) et de plus les entreprises, souvent touchées par ces piratages ne prennent pas conscience de la nécessité de se protéger.

L'utilisation de mots de passe peut être un moyen pour faire obstacle aux intrusions indésirables. Encore faut-il trouver un mot de passe qui ne

(140) Le Monde, 24 fev. 1998

(141) *Internet - enjeux juridiques*, Rapport FALQUE-PIERROTIN, Documentation Française, 1997

(142) "*Introduction à la sécurité sur l'Internet*" Rapport du SCSSI n°2133/SCSSI/SI 12 déc 1997

(143) instruction n°8192/DEF/CAB/CM/3 - BOC/PP 24 mars 1997 n°13

(144) sous peine de sanctions pénales: art. 226-17 C.P.F

sera pas découvert par l'un des logiciels qui peuvent tourner des heures entières pour essayer des mots de passe. Le C.E.R.T *(Computer Emergency Response Team)* estime d'ailleurs que 80 % des intrusions informatiques sont occasionnées par un mauvais choix du mot de passe.

Il faut donc prendre quelques précautions(145). Tout d'abord, modifier régulièrement le mot de passe. Une enquête américaine de 1994(146) révèle que 11% des mots de passe ne sont jamais modifiés et que 90% ne sont pas changés périodiquement. Le choix du mot peut également se révéler important: par exemple, 25% des mots de passe sont des termes triviaux, donc très faciles à découvrir. Il est donc recommandé de choisir des mots de passe d'au moins six caractères, mélangeant les majuscules, minuscules et chiffres, ne constituant pas une séquence de touches de clavier adjacentes ni un mot existant.

Même en respectant ces consignes, l'on n'est pas a l'abri d'une intrusion car il existe des techniques qui permettent de contourner l'obligation de donner son mot de passe.

Les *firewalls* sont des passerelles sécurisées situées entre un réseau local et Internet. Même s'ils ont beau coûté entre 50 000 et 250 000 F, les pirates ne les considèrent pas comme de grands obstacles: "*Ils sont souvent mal utilisés et aussi efficaces que des passoires*"(147).

Il s'agit donc d'améliorer ces parades aux intrusions informatiques et que les entreprises notamment prennent conscience de la nécessité de se prémunir. Comme l'indique le Ministère de l'Intérieur Français(148), la violation de ces moyens de protection permettra de plus de rapporter la trace et la preuve des délits.

(145) *Le monde Internet* Ed. Krol (traduction P. Cubaud & J. Guidon) coll. Guide & Ressources éd. O'Reilly international Thomson 1995

(146) P. ROSE "*Délinquance informatique, inforoutes et nouvelle guerre de l'information*", Cahiers de la Sécurité Intérieure n°24

(147) ANTHONY-CHRIS " Frantic " Zboralski dans " Cyberwars: la montée du crime informatique " Les Echos 10 fev 1998

(148) "*Aspects de la criminalité et de la délinquance en France en 1995*" Ministère de l'Intérieur, La Documentation Française

b) Contre les contenus préjudiciables

La première forme de prévention contre les sites à contenu " illégal et préjudiciable " est sans doute l'information. Cette dernière s'est notamment développée en matière de lutte contre la pédophilie via Internet. Plusieurs sites, de différents pays, alertent les internautes sur ce phénomène(149). La plupart propose de remplir des formulaires en ligne pour faciliter la dénonciation de tels agissements sur le réseau. Ces plaintes seront ensuite transmises aux autorités de police, quand ce n'est pas elles-mêmes qui se chargent de les collecter(150).

Les logiciels de filtrage(151) ont l'avantage de laisser aux internautes la liberté de s'exprimer tout en permettant d'éviter certains dérapages. Ces logiciels permettent en effet de bloquer l'accès à des services dont le contenu peut sembler répréhensible à soi-même ou à ses enfants notamment.

Il en existe une quinzaine sur le marché *(Cyberpatrol, Netnanny, Cybersitter, Cybernanny, SafeSurf, Surfwatch, X-Stop...)* qui filtrent les sites web, les forums de discussion, les bases de données, les moteurs de recherche (le courrier électronique par contre ne peut pas être contrôlé), en fonction des thèmes que l'utilisateur veut exclure.

Ces logiciels utilisent deux méthodes pour contrôler ces services:

La première est d'analyser les mots-clés des sites et de les comparer à ceux prohibés. Certains logiciels possèdent pour se faire des dictionnaires et/ou des agents intelligents d' " évaluation du contexte " pour affiner cette analyse et éviter tout contre-sens.

La seconde méthode, employée en complément de la première, est de faire dresser par des employés naviguant toute la journée sur Internet, des listes noires. Celle-ci permet de répertorier des sites dont le contenu

(149) MAPI (Belgique) **http://www.info.fundp.ac.be/~~mapi/mapi-fr.html**; Pedowatch (Belgique) **http://pedowatch.org/index-f.htm**; Internet Hotline Against Child Pornography (PB) **http://www.meldpunt.org/**; US Customs Service (USA) **http://www.customs.ustreas.gov/enforce/cpep.htm;** Save the Children Norway (Norvège) **http://childhouse.uio.no/redd_barna/**; Internet watch Protection (GB) **http://www.internetwatch.org.uk/hotline**

(150) comme la police belge **http://www.gpj.be**

(151) "*Censorware, la censure privatisée*" Le Monde Cahiers multimédia 12, 13 oct. 1997

n'aurait pas pu être apprécié à juste titre, parce qu'ils contiennent par exemple des photos, qui ne peuvent pas se traduire en mots-clés. Cela implique une mise à jour du logiciel et donc un abonnement de la part de l'utilisateur.

L'avantage premier de ces logiciels est qu'ils permettent aux parents notamment d'éviter que leurs enfants ne consulte des sites à caractère pornographiques, ou faisant l'apologie d'idées contestables..

Mais ces " outils de contrôle parental " font également l'objet de nombreuses critiques. A tel point qu'aux Etats-Unis, on les appelle désormais des " censorware ", c'est-à-dire des " censuriciels ".

La première méthode d'analyse employée aboutit parfois à des aberrations, tandis que la seconde méthode ne peut pas être rectifiée car elle n'a pas pour objet de vérifier les sites exclus (mais ceux qui ne l'ont pas été).Cette analyse conduit à bannir les sites comportant certains termes, sans apprécier l'orientation délictueuse ou non du site. Ainsi, de nombreux sites se sont plaints de voir leur accès restreint parce que les logiciels ne faisaient pas la différence entre un forum consacré aux amateurs des gros seins et celui dédié au soutien psychologique des victimes du cancer du sein.

La seconde méthode d'analyse fait craindre l'arbitraire de la part de l'employé chargé d'établir les listes noires.

Les plus fervents opposants à ces logiciels avancent de plus l'argument selon lequel certaines firmes produisant les logiciels imposent ainsi leur conception de l'ordre moral.

Autre inconvénient, cela pousse les sites à s'auto-censurer, de peur d'être exclus. Enfin, certains font remarquer que ces logiciels de filtrage sont utilisés dans des endroits où les libertés d'expression et d'information ne saurait être limitées. Ainsi, certaines bibliothèques aux Etats-Unis ont installé sur leur poste Internet ces logiciels(152).

Nous allons assister à l'arrivée sur le marché de nouveaux logiciels de contrôle basés sur la norme P.I.C.S *(Platform for Internet Content*

(152) Le Monde 1er nov. 1997; 24 janv 1998

Selection - Plate-forme pour une sélection du contenu d'Internet), élaborée par de grands groupes américains et France Télécom. Ces filtres seront basés sur une notation donnée à chaque site de 1 à 10 relativement à différents thèmes: sexe, violence, haine et chaque internaute fixera son seuil de tolérance pour chacun de ces thèmes. Cette nouvelle forme de logiciels pose également de nombreuses difficultés.

Qui attribuera les notes? Compte tenu de l'impossibilité matérielle pour un organisme extérieur de noter tous les sites qui existent, il a été décidé que chaque serveur s'évaluera.

Qui alors contrôlera que cette notation corresponde bien au contenu du site? Quelles dispositions seront prises à l'encontre des responsables de sites qui n'évalueront pas correctement le contenu de leur site, des responsables qui refuseront ou négligeront de l'évaluer? Il semble que les sites seraient bloqués par tous les types de filtre et exclus des listes fournies par les moteurs de recherche. Un législateur de Washington a déjà même déposé un projet de loi incriminant le fait pour le responsable d'un site de lui attribuer une note trompeuse ou mensongère.

Ce système de notation n'est proposé que dans certains pays (Etats-Unis, France). Les sites des autres pays devront-ils se soumettre à cette notation imposée par quelques pays pour ne pas être inaccessible dans ces derniers?

2) L'auto-réglementation

Elle passe par l'élaboration de codes de bonne conduite **(a)** et l'application de ces codes **(b)**. Ces actions sont soutenues par les instances communautaires[(153)].

a) Les codes de bonne conduite

Le premier code de bonne conduite fut en quelque sorte la Nétiquette et les professionnels prévoyaient déjà l'obligation de la respecter: Désormais, les règles à respecter sur le réseau font l'objet de véritables codes.

(153) Résolution du Parlement du 24 avril 1997, Résolution du Conseil du 17 février 1997, Déclaration de Bonn des 6-8 juillet 1997

Les professionnels d'Internet mettent sur pied, avec l'appui des pouvoirs publics, des codes de déontologie. Cela présente autant d'avantages pour les professionnels que pour les pouvoirs publics: d'un côté, les professionnels évitent une réglementation spécifique par le gouvernement et de l'autre côté, cela garantit aux pouvoirs publics que des règles seront respectées car considérées comme légitimes.

Les exemples deviennent de plus en nombreux.

Ainsi, en France, un groupe de travail présidé par le sénateur BEAUSSANT a présenté le 5 mars 1997(154) à M. FILLON, alors ministre délégué chargé de la Poste, des Télécommunications et de l'Espace une proposition de charte de l'Internet(155). Cette charte a été précédée de réflexions de la part des professionnels.

Cette charte rappelle que les principes du respect de la dignité humaine, des libertés et des droits fondamentaux (secret des correspondances, protection de la vie privée, protection des droits de propriété intellectuelle), de la protection du consommateur doivent être appliqués par les professionnels de l'Internet. Elle propose également la création d'un Conseil de l'Internet, organisme d'autorégulation composé de professionnels. Il aurait pour mission d'émettre des recommandations sur l'évolution de la charte, de conseiller les acteurs du réseau, de les concilier le cas échéant et il pourrait même émettre un avis de suppression ou de blocage à l'encontre d'un site ne respectant pas les dispositions de la charte (après une procédure amiable). Les professionnels souhaitent d'ailleurs que ces avis du Conseil de l'Internet aient une valeur de référence pour l'autorité judiciaire. Ce Conseil de l'Internet ressemble d'ailleurs fort au Comité des services en ligne dont le rapport FALQUE-PERROTIN propose la création.

La charte présentée par M. BEAUSSANT est sans aucun doute inspiré de l'exemple anglais. Le *Service Providers Association (IPSA)* a élaboré l'un des premiers codes de déontologie, qui a donné naissance à d'autres codes, destinés à s'appliquer à des matières plus spécifiques comme le code " R3 Safety Net " de la fondation *Safety-Net* qui lutte contre la pédophilie via Internet.

(154) Y. BREBAN "*Actualité de la régulation de l'Internet*", Gaz. Pal. 13, 15 avril 1997 p.22; " Au fil du Net " Gaz. Pal. 25, 26 juin 1997

(155) **http://www.planete.net/code-internet**

La réflexion sur la charte s'est poursuivie depuis au sein d'un groupe présidé par M. VIVANT, qui a donné naissance à un Manifeste pour l'autorégulation de l'Internet en France(156). Ses auteurs ont tenté de ne pas dépasser les limites de l'autorégulation, critique formulé à l'encontre de la charte. Six missions se dégagent de ce manifeste:

- gérer une ligne d'urgence pour traiter les problèmes de contenus illégaux;
- élaborer des règles ou des réglementations d'usage;
- conseiller les acteurs;
- assurer des fonctions de médiation;
- contribuer à la classification des sites;
- mener des actions de sensibilisation, et de formation aux nouvelles technologies.

b) L'application de ces codes

La pratique révèle que cette coutume est appliquée et on ne peut que s'en réjouir. L'auto-réglementation s'exprime sous la forme d'arbitrage.

Il existe des serveurs qui proposent de régler les litiges entre Internautes(157) et qui ont déjà réglé de nombreux litiges. Les plaignants déposent une plainte expliquant les circonstances du litige et les autres utilisateurs sont invités à donner leur opinion. Evidemment, il ne peut prononcer aucune sanction et sa décision n'a pas force exécutoire, mais dans la mesure où les internautes préfèrent l'autodiscipline à la réglementation étatique, ils ont tout intérêt à suivre ses propositions.

Les internautes peuvent également être invités à voter pour accueillir un nouveau site. C'est ce qui eut lieu en 1996 pour un site spécialisé dans la musique " blanche " et en fait néonazi. Les internautes votèrent par courrier électronique, adressé à un tiers de confiance et refusèrent ainsi la création du site.

(156) "Un nouveau manifeste du droit de l'Internet " interview de D. Kahn Expertises nov. 1997 n° 209 p.339

(157) Virtual Magistrate: **http://vmag.vcilp.org/**, Cybertribunal: **http://www.cybertribunal.org**, Online ombuds Office: **http://www.ombuds.org** ("Les justiciers du Web" Le Monde supplément multimédia 28,29 juin 1998

CONCLUSION

Nous avons traité dans cette étude de certains problèmes légaux et pratiques résultant de l'usage moderne de l'informatique en général et de l'Internet en tant qu'outil de communication en particulier. Cela ne fut pas sans difficultés pratique concernant l'application des idées traditionnelles du droit pénal.

Il est sans doute que l'usage de l'Internet soulève des problèmes pratiques, tel que les crimes de vol et les crimes d'atteinte à la propriété intellectuelle et des droits d'auteurs, ce qui a incité la juridiction américaine et française à combattre ces crimes, domaine dans lequel ces deux juridictions ont excellé. Dans leur combat, les légistes se sont trouvé en opposition aux idées traditionnelles du droit pénal tel que la notion des biens mobiliers dans les crimes de vol.

Notre étude s'est avérée intéressant non seulement la jurisprudence et la juridiction des droits comparés mais également des organisations et associations territoriales. Si le législateur a intervenu dans certains pays pour cadrer légalement l'utilisation d'Internet, il a du se heurter à des obstacles constitutionnels tel que le droit de l'individu à l'expression et à la liberté, mais a certes franchit un pas géant vers la protection des enfants des abus et sévices sexuels. Et en résultat de l'accroissement de l'utilisation d'Internet qui dépasse en terme d'audience les plus diffusées des presses, le législateur a instauré une peine pour les crimes d'injure par Internet.

Les législateurs dans divers pays ont intervenu pour l'instauration de règles juridiques, alors le législateur Koweïtien quant a lui reste immobile malgré le grand besoin de son intervention.

Il est certain que nous souhaitons vivement son intervention mais sans pour autant que cela ne vienne limiter les libertés personnelles d'expression ni d'atteinte aux vies privées des individus.

GLOSSAIRE

- **Adresse**
  Code unique affecté à l'emplacement d'un fichier en mémoire, d'un périphérique dans un système ou dans un réseau ou de toute autre source de données sur un réseau.
- **Adresse IP**
  Adresse codée sur 32 bits selon le protocole Internet et affectée à un ordinateur figurant dans un réseau. Une portion de l'adresse IP désigne le réseau et l'autre désigne un ordinateur dans ce réseau.
- **Autoroute de l'information**
  Mot à la mode qui fait référence au plan du gouvernement Clinton/Gore de déréglementation des services de communication, autorisant l'intégration de tous les aspects d'Internet, de télévision par câble, du téléphone, des affaires, des divertissements, des fournisseurs d'informations, de l'éducation, etc.
- **Bande large**
  Circuit/voie de transmission haute capacité. Elle implique généralement une vitesse supérieure à 1,544 Mégabits par seconde.
- **Bande moyenne**
  Voie/circuit de communications de capacité moyenne. Elle implique généralement une vitesse allant de 64 Kbps à 1,544 Mbps.
- **Base de données**
  Rassemblements d'informations à usage collectif. Permet en général une sélection par accès direct et plusieurs "vues" ou niveaux d'abstraction des données sous-jacentes.
- **BBS (Bulletin board system ou aussi Babillard)**
  Système d'information télématique où les utilisateurs peuvent déposer des messages dans des boîtes aux lettres. De nombreux BBS fonctionnent sur abonnement, payant ou non.
- **Bit**
  Plus petite unité d'information pouvant être transmise. Une combinaison de bits peut indiquer un caractère alphabétique, un

chiffre ou remplir d'autres fonctions parmi lesquelles la signalisation et la commutation.

- **BOT**
  Le terme "bot" (beginning-of-tape, marqueur de début de bande) est couramment employé pour désigner des programmes qui écoutent et répondent à une conversation sur un canal IRC

- **BPS**
  Bits par seconde. Mesure de la vitesse de transmission d'un modem.

- **Canal**
  Voie de télécommunications (canal de transmission) d'une capacité spécifique (vitesse) entre deux emplacements sur un réseau.

- **Capacité**
  Vitesse de transmission (fiable) la plus élevée pouvant être acheminée sur un canal, un circuit ou du matériel. La capacité peut être exprimée en tant que vitesse de base ou débit de traitement net.

- **Cern**
  Laboratoire européen de la physique des particules élémentaires, site de la première conférence du Web et considéré comme le berceau de la technologie du Web. Le travail sur la technologie du Web et l'établissement de standards a été transféré à la World Wide Web Organization (organisation du Web).

- **CGI**
  L'interface Common Gateway Interface (Interface Gateway commune) s'adresse aux programmeurs qui créent des applications ou des scripts exécutés secrètement sur un serveur Web. Ces scripts peuvent générer du texte ou d'autres types de données à la volée, peut-être en réponse à une entrée de l'utilisateur ou à l'extraction d'informations d'une base de données.

- **Compression / Décompression**
  Méthode de codage/décodage de signaux permettant la transmission (ou le stockage) de plus d'informations que le support ne pourrait contenir en temps normal.

- **Conflit enflammé**
  Vive et intense discussion en ligne ignorant les règles établies de la

netiquette. Fait souvent suite à une violation de la netiquette par le destinataire de messages. Flame war.

- **Connexion**
  Voie de transmission point à point spécialisée ou commutée.

- **Cyberespace**
  Employé à l'origine dans le roman Neuromancier de William Gibson traitant de mise en réseau d'ordinateurs intelligents, Cyberespace fait référence aux royaumes collectifs de la communication assistée par ordinateur.

- **Cookies**
  Confidentialité " Cookie ": Certains sites Web mettent en œuvre une technologie dite des "cookies" pour stocker les informations sur vore ordinateur. Ces "cookies" sont généralement utilisés pour assurer les fonctions de personnalisation des sites Web. Avec Internet Explorer 3.0, vous pouvez demander à être prévenu avant le stockage d'un "cookie" sur votre ordinateur, puis choisir d'accepter ou non ce cookie.

- **Dézipper**
  Dé zipper (unzip en anglais) signifie décompresser un fichier dont la taille a été réduite à l'aide d'un utilitaire de compression.

- **Explorateur**
  Logiciel offrant une interface graphique interactive pour rechercher, visualiser et gérer les informations d'un réseau.

- **Fournisseur de services Internet (ISP, Internet service provider)**
  Société qui fournit l'accès à Internet moyennant un abonnement.

- **Finger**
  Protocole permettant de trouver des informations sur les utilisateurs de votre réseau hôte. Certains réseaux ne permettent pas d'utiliser ce protocole à partir d'un système externe et d'autres l'interdisent complètement.

- **FTP (File Transfer Protocol, Protocole de transfert de fichiers)**
  Protocole utilisé pour assurer les transferts de fichiers sur une grande diversité de systèmes.

- **GIF**
  Graphics Interchange Format- Format d'échange de graphiques. Format standard des fichiers image sur le Web mondial. Le format de fichiers GIF est très répandu car il utilise une méthode de compression pour réduire la taille des fichiers.

- **Glisser-déplacer**
  Concept de l'interface utilisateur graphique permettant d'exécuter des actions simples (comme imprimer un fichier, par exemple) en sélectionnant un objet à l'écran et en le déplaçant sur un autre.

- **Gopher**
  Explorateur de base de données publique sur Internet et programme de recherche.

- **GUI**
  Graphical User Interface - Interface utilisateur graphique.

- **HTML (Hyper Text Markup Language)**
  Langage qui permet de présenter et de distribuer les pages web.

- **HTTP (hypertext transfer protocol - protocole de transfert hypertexte)**
  Méthode selon laquelle les documents sont transférés depuis l'ordinateur ou le serveur central vers les explorateurs et les utilisateurs individuels.

- **Hyperlien**
  Connexion entre une information et une autre.

- **Hypermédia**
  Méthode de présentation des informations en unités numériques ou nœuds connectés par des liens. Les informations peuvent être présentées de différentes façons: par exemple, une documentation peut être exécutable seulement ou apparaître comme un texte contenant des graphiques, des sons, des clips vidéo, des animations ou des images.

- **Hypertexte**
  Correspond à un type de navigation en ligne. Les liens (URL) incorporés à des mots ou des phrases permettent d'afficher immédiatement des informations apparentées et des documents

multimédia. L'hypertexte désigne ce type de navigation, où un document en appelle un autre, qui lui-même renvoie sur un troisième, etc.

- **IP (Internet Protocol - Protocole Internet)**
  Protocole Internet qui définit l'unité d'information transmise entre les systèmes et qui fournit un service de distribution de paquets d'informations.

- **JPEG**
  Joint Photographic Experts Group - Technologie de compression de l'image fixe. Méthode courante utilisée pour compresser des images photographiques. La plupart des explorateurs web acceptent les images JPEG comme un format de fichiers standard pour la visualisation.

- **Largeur de bande**
  Mesure de la capacité de communication ou du débit de transmission de données d'un circuit ou d'un canal.

- **Ligne de communication**
  Système matériel et logiciel connectant deux utilisateurs ou plus.

- **Maître/Maîtresse du Web (ou Webmaster)**
  Opérateur/trice du système pour un serveur de site Web.

- **Modem (MODulateur-DEModulateur)**
  Périphérique informatique connecté à un ordinateur et à une ligne téléphonique qui permet de transmettre des données numériques (informatiques) sur une ligne analogique téléphonique). Lorsqu'on émet des données numériques sur la ligne, le modem MODule les données. Lorsqu'on reçoit des données analogiques sur un ordinateur, le modem DEModule.

- **MPEG**
  Moving Pictures Expert Group - Standard de compression des images animées. MPEG est une manière standard de compresser des films vidéos.

- **Multimédia**
  Systèmes informatiques combinant sons, vidéos et données.

- **Naviguer**
  Parcourir le Web en cliquant sur des liens.

- **Numérique**
  Appareil ou méthode qui utilise des variations numériques de tension, de fréquence, d'amplitude, d'emplacement, etc. afin de coder, traiter ou acheminer des signaux binaires (zéro ou un) pour des sons, vidéos, données informatiques ou d'autres informations.

- **Page**
  Document hypermédia sur le Web.

- **Page d'accueil**
  Page de départ d'un site, contenant des informations sur l'identité du propriétaire du site et un index.

- **Passerelle**
  Convertisseur de protocole. Nœud spécifique à l'application qui connecte des réseaux qui seraient autrement incompatibles. Convertit des codes de données et des protocoles de transmission pour l'interfonctionnement.

- **Pointeur**
  Adresse (URL) incorporée dans des données et indiquant l'emplacement de données dans un autre enregistrement ou fichier. Un hyperlien est un exemple de pointeur.

- **"POP" (point of presence - point de présence)**
  Un "pop" est la connexion commutée d'un prestataire de services Internet (ISP) pour les utilisateurs de modem. Il est particulièrement utilisé pour décrire des connexions locales afin que les utilisateurs de modem n'aient pas à composer un numéro longue distance. Ainsi, un ISP spécifique peut être basé à San José mais avoir des "POP" à Los Angeles et New York.

- **PPP (Point to Point Protocol - Protocole point à point)**
  Connexion Internet commutée utilisant le protocole TCP/IP. Le protocole PPP est un peu plus rapide que le protocole SLIP.

- **Privilèges d'accès**
  Privilège permettant d'accéder aux dossiers et de les modifier.

- **Réseau**
  Ensemble d'ordinateurs connectés par une liaison spécialisée ou commutée pour assurer une communication locale ou distante (de voix, vidéos, données, etc.) et faciliter l'échange d'informations entre des utilisateurs ayant des intérêts communs.
- **Robot**
  On parle généralement de "robots" dans le cadre du Web mondial pour désigner des programmes qui parcourent le Web à la recherche d'informations, pour les indexer dans un moteur de recherche ou pour trouver des erreurs dans des sites ou encore pour d'autres raisons.
- **RNIS (Integrated Services Digital Network - Réseau numérique à intégration de services)**
  Ensemble de standards pour la transmission rapide de voix simultanées, de données et d'informations vidéo sur un nombre de canaux inférieur au nombre ordinairement requis, via l'utilisation d'une signalisation hors-bande.
- **Sécurité**
  Mécanismes de contrôle empêchant l'utilisation non autorisée de ressources.
- **Serveur**
  Dans un réseau, ordinateur hôte qui fournit des ressources (zones de stockage, données, programmes, imprimantes, bases de données, etc.) aux autres postes de travail du réseau (appelés clients).
- **Serveur de fichiers**
  Ordinateur assurant l'accès aux fichiers pour les utilisateurs des autres postes de travail du réseau (appelés clients)
- **SGML**
  Le langage SGML (Standard Generalized Markup Language) permet de décrire d'autres langages structurés de description de documents. Par exemple, le langage HTML est défini à l'aide du langage SGML.
- **Signal**
  Changement d'état orienté-objet (par ex. une tonalité, une déviation de fréquence, une valeur binaire, une alarme, un message; etc.).

- **Site**
  Ensemble d'informations structuré stocké sur un serveur Internet.

- **SLIP (Serial Line Internet Protocol - protocole SLIP)**
  Connexion Internet commutée utilisant le protocole TCP/IP.

- **SSL**
  La Secure Socket Layer est un protocole garantissant la sécurité des communications de données par cryptage et décryptage des données échangées.

- **TCP/IP**
  Le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) est le protocole standard de communications de réseau utilisé pour connecter des systèmes informatiques sur Internet.

- **Télécharger**
  transférer des programmes ou des données depuis un ordinateur vers un autre, généralement depuis un serveur vers un poste de travail individuel.

- **Telnet**
  Telnet est un programme réseau qui permet d'ouvrir une session et de travailler sur un ordinateur à partir d'un autre ordinateur. En ouvrant une session sur un autre système, les utilisateurs peuvent accéder aux services Internet dont ils ne disposent pas sur leurs propres ordinateurs.

- **Transporteur**
  Prestataire de services de télécommunications possédant un équipement de commutation de réseau.

- **URL (Uniform Resource Locator)**
  Formulaire de l'adresse du site qui indique le nom du serveur sur lequel sont stoqués les fichiers du site, le chemin du répertoire du fichier et son nom de fichier.

- **Usenet (USEr NETwork - Réseau utilisateur)**
  Groupes de discussion thématiques (Newsgroups) sur Internet. Une des formes les plus récentes de courrier électronique de groupe. On dénombre actuellement environ 30 000 Newsgroups différents.

- **VRML - Virtual Reality Modeling Language - Langage VRML**
  Langage qui permet aux pages Web d'afficher des graphiques tridimensionnels et de proposer un mode de navigation spacial interactif.
- **WAIS (Wide Area Information Server - serveur WAIS)**
  Puissant système permettant de rechercher très rapidement de grandes quantités d'informations sur Internet.
- **World Wide Web (ou toile mondiale)**
  Aussi appelé WWW, le Web est un système d'hypertexte qui vous permet d'afficher des documents en texte au format enrichi (RTF) et des graphiques. A l'aide d'un explorateur Web tel que Internet Explorer, vous pouvez naviguer dans le Web en cliquant sur des liens.
- **WINZIP**
  Winzip est un utilitaire de compression permettant aux utilisateurs de Windows 95, Windows 3.1, et Windows NT de réduire la taille de leurs fichiers pour accélérer la vitesse de transfert sur Internet. Cet utilitaire décompresse également les fichiers ayant été compressés à l'aide des formats PKZIP, LZH, ARJ, ARC ou TAR.

BIBLIOGRAPHIE

1- ouvrages

BENSOUSSAN.M
- *Le logiciel, sous la dir.Forger-on.J.F, Hermés,1994.*

BRUNOT COLL.P
- *La contrefaçon, Que sais-je, Puf, 1986.*

CUBAUD.P&GUIDON.J
- *Le bible Internet, O'reilly Interne-tional Thomson,1995*

FERAL.C
- *Cyber droit, Dalloz, 1999.*

GUISNEL.J
- *Guerres dans le cyberspace, La découverte, 1997.*

HOUNICOUTE.J
- *Internet, Academie international, 1997.*

JAN.C&SABATIER.G
- *La sécurité informatique, Eyrolles, 1989.*

LAFONT.D&MACARY.J.F
- *Le projet Internet F.Alin, Eyrolles, 1997*

LE DORAN.S
- *Les cyber mafias, Rosé, Denoel, 1998*

MARTIN.D
- *La criminalité informatique, Puf, 1997.*

NORTON.B & SMITH.C
- *Understanding business on the internet in week, Hodder&Stought-on, 1997.*

PANSIER F.J
- *La criminalité sur l'Internet, puf, Que sais-je? 2000.*

PRADEL.J
- *Droit Pénal général, Cujas, 2000*

ROSE.P
- *La criminalité informatique, Puf, Que sais-je?, 1988.*

TORTELLO.N & LOINTIER.P
- *Internet pour les juristes, Dalloz, 1996*

2- Articles

BART DE SCHUTTER
- *Propos de la fraude informatique, Rev.dr.pen.crim, 1989.*

COURTOIS.J.P
- *Combattre le piratage de logiciels, Gaz.Pal, 1996.*

HAAS.M.E
- *Les meta-tags comme moyen de générer du trafic sur Internet et la contrefaçon de marques, Gaz.Pal, 1998.*

LENGLART.E
- *L'hébergeur et les amendement, Le monde, supplément nouvelle technologies, 1999*

MARTY.R
- *Marketing pornography on the information superhighway, Georgetown law journal 83, 1995.*

NAIMI.M
- *La problématique des noms de domaine, ou l'attribution des adresses électronique sur web, DIT, 1997*

NICOLEAU.P
- *La protection des données sur les autoroutes de l'information, chron.p, 1996.*

PADOUIN.D
- *La criminalité informatique le role de la police judiciaire, Gaz.Pal, 1996.*

PIETTE-COUDOL.T &BERTRAND.A
- *Internet et la loi, Dalloz, 1997.*

ROSE.P
- *Délinquance informatique info routes et novelle guerre de l'information, Cahiers de la sécurité intérieure.*

OTTAVIO F.
- *La pornographie dure dans l'Internet, Rev.Int. de criminologie et de Police, 1996*

3- Presse

Le Monde

- 9 janvier 1998
  - "*Etude de l'aftel association française de télématique*"
- 23/24 fevier1997
  - "*Internet, l'Europe et la censure*"
- 24 février 1998
- 9 octobre 1997
  - "*Estimation du département du commerce américain*"
- 12/13 octobre1997
  - "*censorware, la censure privatisée*"
- 1er novembre 1997
- 8 novembre 1997
  - "*Bulletin de criminalité informatique*"
- 23/24 novembre 1997
  - "*Le cyber-sexe à nouveau dans la ligne de mire*"
- 26 novembre 1997
- 12 décembre 1997
  - "*le pirate de noël menace Internet d'une bombe à retardement*"

- 12 décembre 1997
  - o "*Les ministres du G8 adoptent un plan d'action contre la criminalité informatique*"
- 20 décembre 1997
  - o "*Etude des instituts Intelli-Quest information group et Zone research*"
- 6 janvier 1998
- 8 janvier 1998
- 17 janvier1998
  - o "*Le quotidien asahi shimbun*"
- 23 janvier 1998
- 25 /26 janvier 1998
  - o "*L'étrange itinéraire médiatique d'un scandale*"
- 1er /2 mars 1998
  - o "*a l'attaque des world companies*"
- 6 mars 1998
  - o "*le pentagone encore visité par les hackers*"
- 28 mars 1998
  - o "*l'analyseur, cambrioleur informatique, devient un héros d'Internet*"
- 21/22 juin 1998
  - o "*trafic sur la toile*"
- 28/29 juin 1998
  - o "*Les justiciers du web*"
- 10 juillet 1998
- 19/20 juillet 1998
  - o "*Ehud tenenbaum, pirate et héros*"
- 16/17 août 1998
  - o "*Sexe, mensonges et internautes*"
- 23/24 août 1998
  - o "*Les quérilleros du xxieme siecle*"
- 9 septembre 1998
  - o "*vers un CDA bis*"
- 16 septembre 1998
  - o "*les pirates de cyberespace s'emparent du New York times*"

Le Figaro

- 21 novembre 1996 — o "*Guerres secrètes sur Internet*"
- 29 novembre 1997 — o "*Cyber-criminalité:la loi du silence*"
- 5 décembre 1997 — o "*la Cyber-flibuste, vent en poupe*"
- 22 décembre 1997 — o "*Les virus informatiques attaquent*"

Les Echos

- 10 févier 1998 — o "*Cyberwars:la montée du crime informatique*"
- 18 décembre 1997 — o "*Les délits boursiers sur l'Internet*"
- 19 janvier 1998 — o "*Les avancées des tribunaux dans le cybermonde*"

Al-Qabas

- 28 juillet 1996 — o "*La protection criminelle de l'informatique*"
- 15 janvier 1997 — o "*La crime informatique*"
- 12 octobre 1998 — o "*Le teux de piratage de logiciel au monde*"
- 8 novembre 1998 — o "*les piratage de l'Internet*"
- 11 septembre 1999 — o "*la liberté sur l'Internet*"
- 11 mai 2000 — o "*Les crimes sur l'Internet*"
- 3 juin 2000 — o "*Le moyen d'age des pirates*"

4- Rapports

- Rapport officiel, G.Théry, *Les autoroutes de l'information*, La Documentation Française 1994

- Rapport au ministre délégué à la Post, aux Télécommunications et à l'Espace et au ministre de la Culture, *Internet-Enjeux juridiques*, La Documentation Française
- Rapport d'information, René Trégouet, *Des pyramide du pouvoir aux réseaux des savoirs*, Commission des finances, Sénat, 1997.
- Rapport intermédiaire, *Contenu illégal et préjudiciable sur Internet*, 4 juin 1997
- Rapport Falque-Pierrotin, *Internet-enjeux juridiques,* Documentation Française, 1997
- Rapport du SCSSI, *Introduction à la sécurité sur l'Internet*, n°2133 / SCSSI/SI, 1997
- Rapport du Ministère de l'Intérieur, *Aspects de la criminalité et de la délinquance en France*, Documentation Française, 1995
- Rapport de la CNIL, Voix, image et protection des données personnelles, Paris, La Documentation Française, 1996

5- Jurisprudence

- TGI Paris, ord.réf, 4 aout 1997, jcp (e) 1997 pan.n° 1021
- TGI Paris, 23 mars 1999, Alice c/ Alice
- TGI Paris, 3e ch, 10 juin 1998, S.D.T. c/EUREVA, sur Cyberlex, note M.Ricouart Maillet
- TGI Paris, 12 juin 1996, Dit 1997/2.
- TGI Paris, 16 Octobre 1991 Gaz.Pal. 1992.I. somm.46
- TGI Draguignan, 21 août 1997
- TGI Nanterre, 18 janvier 1999
- TGI Versailles 22 octobre 1998
- Ca. Paris, 10 février 1999, V.Lacamba c/ E.Hallyday, lp avril 1999, n°160, III
- Crim. 12 octobre 1976 bull. crim.n°287
- Crim. 8 février 1994 Bull. crim.n°58
- Crim.20 févier 1990 D.1991 juris.
- Crim. 8 décembre 1998, bull. crim. déc.1998,n°335

- Décis.n°96-378 DC, Cons. Constit. 23 juillet 1996, jo. 27 juillet 1996
- Decis.n°88-248 DC, cons. Constit. 17 janvier 1988
- Ord.réf. du 9 juin 1998, Estelle lefebure/Valentin lacamba et autres, Epertises,N°219.

6- Webbographie (sites internet)

- http://www.rcmp-grc.ca/html
- http://www.celog.fr/expertises
- http://www.nic.fr/procedures/nommage.html
- http://www.alice.fr
- http://www.argia.fr/Iij
- http://www.2000.ogsm.vanderbilt.edu/rimm.cgi
- http://www.dis.org
- http://www.legalis.net
- http://www.grolier.fr/cyberlexnet
- http://www.aui.fr/Rapports/RAUI070696.html
- http://www.fau.edu/rinaldi.net
- http://www.aclu.org
- http://www.grolier.fr/cyberlex.net
- http://www.culture.fr
- http://www.europa.eu.int
- http://www.meldpunt.org
- http://www.customs.ustreas.gov
- http://childhouse.uio.no/redd_barna
- http://www.internetwatch.org.uk/hotline
- http://www.gpj.be
- http://www.planete.net/code-internet
- http://vmag.vcilp.org
- http://www/cybertribunal.org
- http://www.ombus.org
- http://www.afa-France.com

- http://www.aftel.fr
- http://www.cnil.fr
- http://www.ccip.fr
- http://www.iana.org
- http://www.jurisnet.org
- http://www.senat.fr
- http://www.europa.eu.int/comm
- http://www.zataz.com
- http://www.anti-hack.org
- http://www.truste.com