TABLE DES MATIERES

1

TITRE PREMIER. 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.

Cet essor d'Internet en France est nécessaire car ce nouvel outil de communication est le précurseur d'une nouvelle société ; celle des autoroutes de l'information selon la formule du Vice-Président américain Al Gore. Ces autoroutes 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 "[2]. Selon Olivier Quéau, directeur de la division informatique et information de l'UNESCO [3] : " 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[4]. 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.

Les Français se doivent de maîtriser les techniques indispensables à l'utilisation et la création de ces réseaux : dans leur intérêt individuel s'ils ne veulent pas faire partie des exclus de cette société ; dans l'intérêt du pays si la France veut rester une forte puissance.

Conscient de l'enjeu économique et culturel que peut représenter cette nouvelle forme de communication, le gouvernement français favorise le développement de cet outil. Certes, il y a en France un million d'utilisateurs dont entre 250 000 et 300 000 abonnés individuels[5], mais les Etats-Unis en comptent plus de 40 millions (soit dix fois plus, rapporté au nombre d'habitants), dont 47°/. de femmes[6]. Le Premier Ministre Lionel Jospin a ainsi annoncé la mise en marche de l'action du Gouvernement pour préparer l'entrée de la France dans la société de l'information le 25 août 1997,par ce qui restera sous le nom de " discours d'Hourtin ".

L'objectif est double. Il tout d'abord s'agit de motiver les entreprises du secteur des technologies de l'information et de la communication à s'investir pour que la France devienne un " pays –moteur " de la société de l'information. Il s'agit surtout de faire prendre conscience aux particuliers du formidable outil que leur offre le multimédia et dont il faudra savoir se servir pour participer au monde de demain. 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 ".

1

[2]Rapport Officiel *Les autoroutes de l'information* - G. Théry - La Documentation Française 1994 - p.14
[3]Émission : " Allô la terre - les autoroutes de l'information " - La Cinquième - du 17 au 20 nov. 1997
[4] le Rapport Officiel *Les autoroutes de l'information* par G. Théry (p.61 &s.) contient de nombreux exemples
[5]selon une étude de l'Aftel (Association française de télématique) - Le Monde 9 janvier 1998
[6]selon une étude des instituts Intelli-Quest Information Group et Zona Research - Le Monde 20 décembre 1997
[7]Émission : " Allô la terre - les autoroutes de l'information " - La Cinquième - du 17 au 20 nov. 1997

Mais toute grande invention présente un effet néfaste quand elle est mal utilisée. Ainsi l'imprimerie favorisa l'essor de l'instruction mais permit également la diffusion d'idées critiquables. Dans le cas d'Internet, les risques de détournements sont plus grands dans la mesure où ce réseau permet des utilisations diversifiées. Pour comprendre la délinquance qui peut y être associée, il faut alors étudier plus précisément son fonctionnement, ce qui nécessite, pour une meilleure appréhension de connaître son histoire.

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'ARPA (Advanced Research Pojects Agency - l'agence de recherche du Ministère américain de la Défense) qui mit au point le premier réseau : l'ARPAnet (c'est à dire le " réseau de l'ARPA ").

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 NCP (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. 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 noeud (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. Dès lors, l'existence de l'Internet ne tenait plus qu'à la participation au réseau du plus de noeuds 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 finançant la recherche) créa ce qui fut sans doute le plus grand réseau de l'époque : le NSFNET qui intégra ARPAnet. La France s'y connecta en 1988.

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 newsgroups. La France créa dans le même but en 1992 RENATER (le Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) à partir de réseaux universitaires, puis régionaux .

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'araigné 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 Nestcap, des logiciels qui permettent à tout profane de naviguer simplement sur la toile (ce sont des *browsers* ou "butineurs ", " navigateurs ")

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 relié matériellement les uns aux autres pour pouvoir s'échanger des informations. Ces liens peuvent être de quatre ordres : soit des câbles téléphoniques, soit des câbles 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 dôté 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 quatre en France : RENATER, Transpac, Oléane et Eunet), 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.

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[8]), 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 .

[8] selon une estimation du département du commerce américain Le Monde 9 oct. 1997

- la facilité de lecture du message : le destinataire peut utiliser n'importe quel ordinateur (et maintenant même un Minitel) pour ouvrir sa boîte à lettre.
- l'utilisation du message : le message peut être lu sur l'écran, conserver, imprimer, envoyer 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.

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[9], dont les thèmes sont aussi divers que nombreux, voire discutables comme la pédophilie ou le révisionnisme. 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 un pirate informatique qui désirait 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 ...) . Il 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'internaute découvre 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.

C'est la nouveauté et la pluralité de ces 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[10] 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

[9] " Internet, la toile d'araignée informatique " Armées d'aujourd'hui n°227 févr 1998 p.65
[10] 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

quasi-totalité des comportements condamnables (Titre 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 (Titre II) .

TITRE DEUXIÈME. LA TECHNIQUE DE LA REPRESSION

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 émettre des informations

De ce fait, on peut distinguer deux grands types de comportement 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 chapitres suivants 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.

Comme nous l'avons laissé entendre, le droit français est à même de réprimer ces comportements. 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 : dans la première hypothèse, Internet n'est que le support d'une information contestable, comme il en existe d'autres (Chap. I.) tandis que dans la seconde hypothèse, il porte atteinte à une information ; cette dernière devient l'objet de l'infraction (Chap. II.).

CHAP. I. L'INFORMATION, VECTEUR DE L'INFRACTION

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 a déjà pris des dispositions à l'égard de ces derniers, dispositions qui sont dès lors, susceptibles de s'appliquer à Internet.

Le droit pénal peut ainsi appréhender les auteurs d'infractions dans lesquelles une information est l'un des faits constitutifs de celles-ci parmi d'autres (Sect°. I) et les auteurs d'infractions constituées par l'émission, la divulgation d'une information particulière (Sect°. II).

SECT°. I. L'INFORMATION REPREHENSIBLE DANS UN CONTEXTE

Dans certaines hypothèses, l'information va concourir à un comportement délictueux. Ce peut être notamment le cas dans le cadre de propositions commerciales (§1), ou de la messagerie (§2).

§1. LES PROPOSITIONS COMMERCIALES

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[1]. Une société new-yorkaise avait créé deux sites d'images 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 CP 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* ".

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[2].

B. LA VENTE

Les opérations de ventes seront certainement l'occasion de pratiques douteuses. Ces dernières risquent de se développer parallèlement au commerce électronique.

I. LA VENTE A LA BOULE DE NEIGE

Ont déjà été mises à jour des ventes à la boule de neige. Une province australienne a par exemple relevé l'existence de 200 sites proposant des pyramides financières, auxquels elle a adressé un avertissement[3]. Aux Etats-Unis, la Cour fédérale du district de Washington ne s'est pas contenté d'un simple avertissement. Elle a rendu une ordonnance d'interdiction définitive du site de la société Fortuna Alliance qui servait à la promotion et au développement d'un système de vente pyramidale[4]. Rappelons que la loi française par l'art. L. 122-6 CCons° interdit " *le fait de proposer à une personne de collecter des adhésions ou de s'inscrire sur une liste en lui faisant espérer des gains financiers résultant d'une progression géométrique du nombre des personnes recrutées ou inscrites* ", comportement sanctionné d'un an d'emprisonnement et d'une amende de 30.000 frs selon l'art. L. 122-7 CCons°.

II. LA VENTE DE PRODUITS INTERDITS

[1] Le Monde 8 nov. 1997 – Bulletin de la criminalité informatique (Canada) avril 1997 http://www.rcmp-grc.ca/html
[2] Selon le quotidien Asahi Shimbun Le Monde 17 janv. 1998
[3] Le Monde 22 oct. 1997
[4] Cet société diffusait à travers 60 pays le message " que diriez-vous de payer 250 $ par mois qui produiront un revenu minimum mensuel de 5 250 $. Cette vente pyramidale fit 17 000 victimes, ayant payer entre 250 et 1 750 $ chacune. *Les cyber mafias* S. Le Doran & P. Rosé éd. Denoël 1998 p. 216 - Gaz. Pal. " Au fil du Net " 6, 8 avril 1997

Nous laisserons de côté la vente de stupéfiants, d'armes ou de faux documents[5] pour nous en tenir à deux exemples : les médicaments (1) et les contrefaçons (2).

1. Les médicaments

La presse s'est récemment émue[6] de la facilité avec laquelle l'on pouvait acquérir par le biais d'Internet des médicaments disponibles uniquement sur ordonnance, souvent soumis à une réglementation très sévère, tels des hormones de croissance, des psychotropes, des médicaments anorexigènes ou cardio-vasculaires, des médicaments n'ayant pas reçu d'autorisation de mise sur le marché[7], voire des médicaments périmés, sans étiquette ou sans mode d'emploi. La majorité des serveurs proposant ces produits se situent pour l'instant aux Etats-Unis, aux Pays-Bas et en Suisse. L'Organisation Mondiale de la Santé s'est inquiétée lors de son assemblée générale de mai 1997[8] " *de ce que la publicité, la promotion et les ventes par Internet risquent de déboucher sur un commerce transfrontières incontrôlé de produits médicaux susceptibles de ne pas être évalués ni approuvés et d'être dangereux ou inefficaces ou encore d'être mal utilisés* " et des responsables de l'industrie pharmaceutique réclament des mesures internationales.

A l'échelon national, ces ventes seraient susceptibles de faire l'objet de poursuites sous le chef d'exercice illégal de la pharmacie. En effet, l'art. 517 Code de la Santé Publique puni d'une amende de 30.000 frs " *quiconque se sera livré sciemment à des opérations réservées aux pharmaciens sans réunir les conditions exigées pour l'exercice de la pharmacie* " Il faut ajouter que cette disposition est également applicable à celui qui n'a pas la qualité de pharmacien et proposerait à la vente des produits qu'il présente comme des médicaments et qui ne le sont pas[9]. On pourrait ainsi poursuivre ceux qui par le biais d'Internet proposent des remèdes miracles, à défaut de les poursuivre pour escroquerie ou publicité mensongère. Notons qu'un groupe de travail regroupant des associations américaines, canadiennes et mexicaines a dénombré fin 1997 plus de 400 sites proposant des "médicaments" contre le cancer, le sida, l'arthrite, le diabète, ou la sclérose en plaque[10].

2. Les contrefaçons

Internet peut également être le support de la vente de produits contrefaits, quelqu'en soit la nature. Le réseau étant utilisé majoritairement par des gens qui s'intéresse à l'informatique, la vente de logiciels 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 "[11] 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 prise 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 Lorrains 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[12].

Or, la contrefaçon de logiciel est très préoccupante[13]. 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%[14]. 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, il pénalise l'emploi[15]. Toutes ces constatations sont relatives à

[5] " Trafic sur la Toile " Le Monde supplément multimédia 21,22 juin 1998 – " Passeports à vendre " Le Monde 3 sept 1998
[6] Le Monde 4 oct. 1997
[7] Voir l'exemple du Viagra Le Monde 30 juin 1998
[8] Gaz. Pal " Au fil du Net " 23, 24 juill. 1997
[9] CAp Colmar – 18 juin 1982 (inf. pharm. 1983. 44) à propos d'un individu qui vendait des baumes, poudres, ou lotions présentées comme ayant des propriétés curatives ou préventives des maladies humaines.
[10] Le Monde 11 nov 1997
[11] *La contrefaçon* P. Brunot coll. QSJ éd.PUF 1986
[12] panorama de presse du SEFTI – 1er trimestre 1996
[13] " Combattre le piratage de logiciels " J.P. Courtois Gaz. Pal. 12, 13 juin 1996 p.36
[14] 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
[15] 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.

l'ensemble des formes de piratage de logiciels, et on peut penser qu'Internet et sa facilité d'utilisation ne feront qu'accroître ce phénomène.

C'est pourquoi le logiciel est protégé[16] au même titre que les autres œuvres de l'esprit énumérées par l'art. L.112-2 Code de la Propriété Intellectuelle. 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 CPI) par contre, l'art. L.335-3 CPI 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[17] 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 CPI) 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.

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 $.

C. LES PRESTATIONS DE SERVICES

A l'image de la vente, certaines prestations de services peuvent être concernées. Ainsi, les serveurs proposant des jeux de hasard (I.), des services bancaires (II.) ou les " serveurs-roses " (III.) se révèlent parfois proposer des services délictueux.

I. LES CASINOS

Les casinos virtuels représentent de nombreux sites[18]. Un rapport rendu au Congrès par le sénateur américain Richard Lugar en dénombrait fin 1996 200 en activité[19]. Certains ne concernent que des mises peu importantes[20], mais d'autres acceptent des paris allant de 10 à 15.000 dollars. D'ici l'an 2000, le marché des casinos virtuels atteindrait 40 milliards de dollars par an. En France, la tenue de jeux de hasard fait l'objet d'une réglementation stricte édictée par la loi du 12 juillet 1983 qui prévoit à l'égard de ses contrevenants des sanctions pénales.

II. LES PRATIQUES BANCAIRES

Dans le même genre d'idée, Internet peut favoriser des relations commerciales peu regardantes. Ainsi, une banque installée sur Internet sera sans doute moins exigeante quant à la probité de ses clients. L'European Union Bank[21], créée en 1994 à Antigua, et fermée depuis l'été 1997 après que ses créateurs aient disparu (avec les avoirs de la banque bien sûr..), proposait des comptes dont seul le titulaire connaît le numéro et permet de passer d'une devise à une autre. Ce type d'établissement, s'il facilite la tâche du contribuable qui veut s'adonner à l'évasion fiscale sans se déplacer, permet également de blanchir de l'argent[22] issu de trafics en tout genre.

Les établissements bancaires facilitant les opérations de blanchiment, qu'ils soient réels ou virtuels, se situent dans les mêmes paradis fiscaux où ils profitent d'un lourd secret bancaire et d'une législation peu répressive : les Bahamas, les Iles Caïman, le Mexique. Mais Internet a un avantage considérable pour celui qui veut blanchir de l'argent, et l'on peut craindre que le milliard de dollars qui se blanchit chaque jour sur les

[16] *Le logiciel et le droit* Mémento guide Bensoussan sous la direction de J.F. Forgeron éd. Hermès 1994
[17] Depuis la loi n° 94-102 du 5 février 1994
[18] http://www.casino.org/
[19] *La criminalité informatique* D. Martin p. 43 éd. PUF – coll. Criminalité internationale
[20] citons le cas d'un site espagnol proposant, avant que la police espagnole ne le ferme, un jeu de bingo rassemblant plusieurs centaines de joueurs qui misaient des sommes allant de 8 à 800 frs – Le Monde 25 nov. 1997
[21] *La criminalité informatique* D. Martin p. 38 éd. PUF – coll. Criminalité internationale
[22] *Les cyber mafias* S. Le Doran & P. Rosé éd. Denoël 1998 p. 238 & s.

marchés financiers mondiaux[23] ne transite désormais par Internet ou ne représente une somme plus importante. En effet, le commerce électronique est l'atout des réseaux. Désormais, les *schtroumpfs* déposeront l'argent sale dans différents comptes de différentes banques, puis celui qui souhaite blanchir son argent le transféra, du guichet virtuel de la banque où il est déposé vers le guichet virtuel d'une autre banque et pourra multiplier ce type d'opérations. L'argent sera ainsi devenu de la monnaie électronique, monnaie qui pourra être utilisée pour des paiements sans limitation de frontière, monnaie totalement anonyme, comme le numéraire.

III. LES SERVEURS DE CHARME

Il existe de nombreux serveurs de charme proposant leurs services sur Internet.
Si la prostitution n'est plus une infraction en France, le racolage et surtout le proxénétisme le sont. Mais les services proposés par les serveurs de charme sont-ils susceptibles de constituer ces infraction ?

1. Le racolage

Le racolage, qui est le fait selon l'art. R. 625-8 CP " *par tout moyen, de procéder publiquement au racolage d'autrui en vue de l'inciter à des relations sexuelles* " constitue une contravention de la 5ème classe.

La conception traditionnelle de cette infraction tend à incriminer la prostitution active, dans les lieux publics. Si les juridictions venaient à considérer que l'adverbe " publiquement " ne vise pas seulement une action sur la voie publique mais toute action faisant l'objet d'une publicité, et que l'on considère que certains services d'Internet ont un caractère public, peut-être que les " hôtes " ou " hôtesses " de certains services de " charme " pourrait être considérés comme faisant du racolage.

2. Le proxénétisme

Le proxénétisme se définit dans sa conception traditionnelle comme le fait " *de tirer profit de la prostitution d'autrui, d'en partager les produits ou de recevoir des subsides d'une personne se livrant habituellement à la prostitution* " selon l'art. 225-5-2° CP.

Or a chambre criminelle considère dans son dernier état[24] que la prostitution constitue le fait " *de se prêter, contre rémunération, à des contacts physiques de quelque nature qu'ils soient, afin de satisfaire les besoins sexuels d'autrui* ". De ce fait, les personnes qui travaillent pour les serveurs de charme ne peuvent pas être considérées comme des prostitué(e)s.
Par voie de conséquence, les responsables de ces serveurs ne sont pas des proxénètes puisqu'ils ne mettent pas en contact des prostitué(e)s et des clients puisqu'ils n'y a pas prostitution.

Il demeure que les responsables de ces serveurs gagnent des sommes importantes grâce à leurs " hôtes " et " hôtesses ", qui sont peut-être parfois dans la même situation de dépendance vis à vis de leur employeur que les prostituées. Il n'est peut-être pas bon d'étendre le champ d'application du proxénétisme, mais il est intéressant à noter qu'une autre définition de la prostitution, déjà employée, aurait pour effet d'incriminer les actes de ses serveurs.

Certaines juridictions[25] définissent selon l'application d'une jurisprudence de 1912[26] la prostitution comme le fait " *d'employer, contre rémunération, son corps à la satisfaction des plaisirs du public, quelle que fut la nature des actes de lubricité* ", comme par exemple " *le fait d'exhiber ses parties sexuelles* ". Si la jurisprudence revenait à ce type de conception où le contact physique ne serait pas exigé, on pourrait considérer que sur de nombreux serveurs " de charme " (ainsi que sur d'autres supports) ainsi que sur les nouveaux services dont le progrès à venir nous réserve la surprise, se trouveraient des personnes se livrant à la prostitution. De ce fait, les responsables des serveurs en question seraient des proxénètes au sens de l'art. 225-5-2° CP, et peut-être même coupables de proxénétisme hôtelier, si l'art. 225-10 CP recevait une interprétation large.

Jusqu'à présent, il n'y a proxénétisme que si les personnes que l'on voit sur ces services se livrent " physiquement " à la prostitution et que le service propose de les rencontrer dans ce but. Servir d'intermédiaire peut se faire par Internet, de la même manière que l'on peut servir d'intermédiaire en diffusant dans son journal

[23] selon Pino Arlacchi, spécialiste de la criminalité organisée – Soirée Théma " Internet " Arte 20 mars 1998
[24] Crim. 27 mars 1996 Bull. Crim. n°138
[25] la Cour d'appel dans l'affaire qui a donné lieu à l'arrêt du 27 mars 1996
[26] Civ. 19 nov. 1912 DP. 1913 .1. 353

des annonces d'offres manifestement prostitutionnelles[27]. Il y a alors proxénétisme selon l'art. 225-6–1° CP. Il y a d'ailleurs déjà eu un précédent dans un domaine proche, celui des messageries sur Minitel[28]. La personne responsable pénalement est dans ce cas soit la personne morale qui gère le serveur (art. 225-19 CP), soit l'un des responsables du serveur.

Enfin, le proxénète peut être celui, selon l'art. 225-5-3° CP qui embauche, entraîne ou détourne une personne en vue de la prostitution. Cette infraction est constituée notamment par la publication de petites annonces dans des journaux[29]. Cette solution est transposable à des petites annonces diffusées sur Internet. Le nouvel art. 225-7 CP, issu de la loi du 17 juin 1998[30] confirme d'ailleurs cette affirmation : l'utilisation d'un réseau de télécommunications (le Parlement visant expressément dans ses travaux Internet) par le proxénète pour entrer en contact avec sa victime devient une circonstance aggravante.

§2. LA MESSAGERIE

Internet est un moyen privilégié de communication pour les délinquants.

En effet, il présente de nombreux atouts pour des informations relatives à leurs activités.

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[31] 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 stéganographie[32] 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 uns de ces chiffres 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[33]. 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[34].

---

[27] Crim. 9 oct 1996. Bull. Crim. n°355
[28] Trib. Corr. Paris 9 oct. 1997 aff 3615 Aline – Expertises n°210 déc. 1997 p.374
[29] Crim. 15 avril 1975 Gaz. Pal. 1975. II. 505
[30] 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
[31] voir " la cryptologie " p.86
[32] *Les cyber mafias* S. Le Doran & P. Rosé éd. Denoël p. 60 – *La criminalité informatique* D. Martin éd. PUF p. 42
[33] *Les cyber mafias* S. Le Doran & P. Rosé éd. Denoël p.44
[34] *La criminalité informatique* D. Martin éd. PUF p42

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 CP énonce que " *constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation, 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 CP 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 CP) 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 CP).

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 a admis en 1990[35] 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, quelqu'en soit la forme, via Internet pourrait constituer un acte préparatoire déterminant.

Nous pouvons faire trois remarques en conclusion.

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 [36] 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[37], les personnes morales peuvent être déclarées pénalement responsables de l'infraction (art. 450-4 CP) et encourt 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.

SECT°. II. L'INFORMATION REPREHENSIBLE EN ELLE-MÊME

Certaines informations qui circulent par Internet sont constitutives d'infraction en raison de leur existence même. Ce type d'information est aussi diversifié que celle de la catégorie précédente. Nous pouvons les regrouper dans deux catégories : certaines informations sont incriminées essentiellement afin de protéger la société dans son ensemble (§.1) tandis que d'autres visent à protéger les membres de cette société individuellement (§.2).

[35] Crim. 20 fév 1990 D.1991 Juris. P.395

[36] Crim. 20 fév 1990 D.1991 Juris. P.395 – TCorr Paris 16 oct 1991 Gaz. Pal. 1992.I. somm.46

[37] 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

§1. LA PROTECTION DE LA SOCIETE

Afin de protéger la société, certains messages comme ceux présentant un caractère sexuel (A.), provocateur (B.) ou violant un secret (C.) constituent des infractions.

A. LES MESSAGES A CARACTERE SEXUEL

La diffusion de messages à caractères sexuel[1] est sans doute le principal vice que les média 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 *Time Magazine*[2] révéla en 1995 que 83,5 % des forums comprenaient des images pornographiques tandis qu'une autre étude[3], 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[4]. Ceux-ci diffusent des images, des films pornographiques, proposent à la vente du "matériel". Certains IRC permettent des discussions érotiques. Toutes ces activités ne sont pas illicite car la pornographie n'est pas interdite en elle-même. Elle n'est prohibée que dans certaines hypothèses en fonction de son mode de diffusion (I.) ou de son objet (II.).

I. LA PORNOGRAPHIE PROHIBEE EN RAISON DE SON MODE DE DIFFUSION

Lorsque son mode de diffusion la rend susceptible d'être vue ou perçue par le public (1.) ou par un mineur (2.), la pornographie devient interdite.

1. La pornographie diffusée publiquement

La pornographie peut être poursuivie sous le dénomination " indécence " lorsque sa diffusion est publique. En effet, l'art. R. 624-2 CP prévoit que " *le fait de diffuser sur la voie publique ou dans des lieux publics des messages contraires à la décence est puni de l'amende prévue pour les contraventions de la 4ème classe. Est puni de la même peine le fait, sans demande préalable du destinataire, d'envoyer ou de distribuer à domicile de tels messages* ".
Nous voyons que ce texte ne pourra s'appliquer à Internet que dans la mesure où le service concerné sera public. Cependant, l'alinéa second peut s'appliquer sans aucun doute au messages qui seraient distribuer dans des e-mails qui ont très certainement le caractère de correspondance[5].

---

[1] " Pornography on the Internet " Yaman Akdeniz http://www.argia.fr/lij – " 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 " I. Ottavio Francescon Rev. Int. de Criminologie et de Police 1996 n°1 p. 61
[2] Philip Elmer-Dewitt "On a screen near you: Cyberporn" [1995] Time, July 3, 34-41. 5. – d'après une enquête Marty Rimm "Marketing Pornography on the Information Superhighway" [1995] Georgetown Law Journal 83, 1839-1934.
[3] Par MM. Hoffman et Novak - http://www2000.ogsm vanderbilt.edu/rimm.cgi.
[4] Quelques exemples de forums relatifs à la sexualité à connotation : scatologique " alt.binaries. pictures. erotica. tasteless " - nécrophile " alt.sex.necrophilia " - zoophile "alt.sex.zoophilia "
[5] Il est intéressant de relever deux particularités de ce texte. Cet article prévoit la responsabilité des personnes morales, alors que le texte que nous étudierons ensuite ne la prévoit pas, ce qui est curieux puisque l'art. R.624-2 vise une contravention tandis que l'art. 227-24 vise un délit. De plus, seul l'art. R. 624-2 prévoit comme peine complémentaire la confiscation de la chose qui a servi ou était destinée à commettre l'infraction. Pourtant cette peine serait efficace dans la seconde hypothèse que nous allons étudier et se justifie plus en matière correctionnelle que contraventionnelle.

2. La pornographie diffusée au mineur

Ce qui est interdit, c'est de permettre à des mineurs de visionner ce type d'images. C'est la raison pour laquelle la presse enfantine est soumise à des obligations strictes ainsi que la presse pornographique. La loi du 17 juin 1998[6] a d'ailleurs renforcé cette réglementation. Le législateur veut éviter une "mise en péril " morale du mineur, pour reprendre l'intitulé du chapitre dans lequel figure l'interdiction.

L'art. 227-24 CP réprime en effet "*le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit le fait de faire commerce d'un tel message../..lorsque ce message est susceptible d'être vu ou perçu par un mineur* ", comportement puni de 3 ans d'emprisonnement et de 500 000 F d'amende.

Remarquons tout d'abord qu'il n'y a aucune condition quant au moyen de communication permettant la diffusion du message. Pour donner un aperçu des différents types de supports concernés, on peut se référer à la liste énoncée par l'art. 283 de l'ancien Code Pénal en matière d'outrage aux bonnes mœurs : imprimés, écrits, dessins, affiches, gravures, peintures, photographies, films, clichés, matrices, reproductions phonographiques, emblèmes Ce texte a donc vocation à s'appliquer à Internet, à condition que soient réunis les trois éléments constitutifs de l'infraction.

- L'action : fabriquer, transporter, diffuser, faire commerce…

  Cette incrimination permettrait de poursuivre diverses personnes.

Celui qui aura "fabriqué" le message peut tomber sous le coup de cet article. On peut imaginer que l'article s'appliquera tant à celui qui prendra la photo, créera le texte condamnable, qu'à celui qui participera à sa fabrication directement.

Concrètement, prenons l'exemple d'une photographie pornographique diffusée sur Internet. On peut considérer qu'au moins deux personnes sont intervenues dans la fabrication de cette image : le photographe tout d'abord, qui a matériellement pris la photo, puis celui qui a scannérisé la photographie pour qu'elle devienne une image lisible par l'ordinateur (évidemment, ces deux personnes peuvent en être une seule, surtout si le matériel photographique est directement connecté à l'ordinateur).

Celui qui " transporte " le message. Sous ce terme curieux l'on pourrait viser diverses catégories de personnes. La jurisprudence aurait tout intérêt à définir ce transport. Il pourrait concerner celui déplace d'un endroit à un autre le message, c'est à dire un fournisseur d'accès, un opérateur ou l'internaute qui rapatrierait le message sur son ordinateur. A la condition évidemment d'en avoir l'intention selon le principe de l'art. 121-3 CP.

Celui qui " diffuse " le message. Cette diffusion peut se faire par quelque mode que ce soit, donc y compris par les réseaux. Il faut d'ailleurs noter que lorsque la diffusion se fait par voie de la presse ou de l'audiovisuel, les principes particuliers de responsabilité s'appliquent. La question se posera de savoir si cela vise non seulement l'éditeur de contenu mais également son fournisseur d'hébergement et les fournisseurs d'accès qui permettent l'accès au message.

Celui qui en " fait commerce ". La jurisprudence devra également définir cette activité car on peut se demander qui est susceptible de faire commerce du message sans ni le fabriquer, ni le transporter, ni le diffuser. Peut-être le législateur a-t-il voulu viser ceux qui seraient à la tête de sociétés ou organisation diffusant ces messages.

- L'objet : un message à caractère violent, ou pornographique ou de nature à porter gravement atteinte à la dignité humaine

  Cet article ne s'applique pas qu'aux messages pornographiques : il a vocation à s'appliquer dès lors qu'est diffusé (ou fabriqué…) un message de nature à porter gravement atteinte à la dignité humaine, dont le message violent ou pornographique ne sont que des exemples. Notons que le texte exige que le message porte **gravement** atteinte à la dignité humaine, cette condition ne semblant pas s'appliquer aux messages particuliers de violence et de pornographie (soit parce que le législateur considère que tout message violent ou pornographique implique la gravité, soit parce qu'il considère que ces types de messages sont particuliers).

En matière de message pornographique, il n'y a donc pas de condition de particulière gravité. Cet article concerne alors aussi bien la "simple" pornographie que la "pornographie dure"[7] que l'on peut définir à l'instar de l'art. 197 du Code Pénal suisse comme celle qui a pour contenu des actes d'ordre sexuel avec des enfants, des animaux, des excréments humains ou comprenant des actes de violence. Nous pouvons d'ailleurs relever que certains de ces types de pornographie tomberont sous le coup d'autres dispositions pénales.

---

[6] art. 32 à 39 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

[7] – " 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 " I. Ottavio Francescon Rev. Int. de Criminologie et de Police 1996 n°1 p. 61

- La probabilité que le message soit vu ou perçu par un mineur

Cette condition est essentielle, elle constitue la raison d'être de l'incrimination.

Différentes remarques doivent être faites. Tout d'abord, il faut souligner qu'il n'y a pas de condition relative au mineur concerné : il peut donc avoir moins ou plus de 15 ans. De plus, le texte n'exige pas que le message ait été vu ou perçu. Il suffit que cela soit possible. Cette précision permet d'élargir l'incrimination.
Se pose alors la question de savoir si tout message qui circule sur Internet doit être considéré comme susceptible d'être vu ou perçu par un mineur. Si l'on estime que ce n'est pas le cas dans certaines hypothèses où le message n'est accessible que sous certaines conditions, il faudra établir qu'elle sous les conditions suffisantes. La jurisprudence parle *de "conditions permettant d'en limiter la diffusion aux seuls adultes"*[8]. La question revient à celle du caractère public ou privé du message.

II. LA PORNOGRAPHIE AYANT POUR OBJET UN MINEUR

C'est par cette matière que la dangerosité d'Internet a été découverte.
Certaines associations de défense de l'enfance (End Child Prostitution in Asian Tourism) avancent le chiffre d'un million d'images pornographiques et 40 millions de pages Internet consacrées à la pornographie enfantine[9].

Les pédophiles utilisent en effet Internet pour visionner des films, des photographies pornographiques de mineurs. La plupart de ces images sont accessibles sur certains forums de discussion dont le nom est parfois très évocateur, le plus connu étant "Alt.Sex.Pedophilia" qui a été fermé[10]. Souvent, la condition préalable à la consultation des images apportées par les autres connectés est de proposer à l'échange ses propres images. Ces lieux d'échange permettent également de proposer à la vente certains matériels ou de passer des petites annonces. Considérées comme assez limitées, ces ventes rapporteraient selon une estimation[11] du Ministère américain de la Justice entre 2 et 3 milliards de dollars par an. De nombreux sites web ont également cette activité. Les premières photos ou vidéos sont téléchargeables gratuitement, puis les autres sont payantes, ainsi que l'envoi de CD-Rom, de vidéos, la participation à un voyage[12]…

Si le Code Pénal ne réprime pas la pornographie, il la sanctionne lorsqu'elle représente des mineurs, le législateur voulant protéger ces derniers à deux niveaux : Il s'agit d'éviter tout d'abord que celui qui collectionne ce type de représentations ne concrétise son fantasme. De plus, l'existence de cette incrimination tend surtout à éviter que des mineurs soit contraints de poser pour ces images. En effet, il ne faut pas oublier que l'existence de ces images implique souvent (avec les progrès de la technique, les représentations virtuelles se multiplieront) que des mineurs aient " posé " pour ces photos et films. Ces enfants auront été le plus souvent contraints à cette participation, sous la menace et la réalisation de violences physiques, sexuelles et psychologiques. L'incrimination permet de poursuivre ceux qui auront fait prendre ces photographies lorsque l'on ne pourra pas rapporter la preuve qu'ils ont personnellement contraint des mineurs à se livrer à ce type d'activité. Bien sûr, si cette preuve peut être rapportée, des poursuites cumulatives pour corruption de mineur (art. 227-22 CP) seront possibles.

Cette répression est assurée par l'art. 227-23 CPP qui a connu une modification récente, notamment à la suite de la prise de conscience des activités de certains internautes. Dans sa nouvelle rédaction, issue de la loi du 17 juin 1998[13], l'art. 227-23 énonce que : " *le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de 3 ans d'emprisonnement et de 300 000 F d'amende. Le fait de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter est puni des mêmes peines. Les peines sont portées à 5 ans d'emprisonnement et à 500 000 F d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunications. Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un*

[8] Crim. 29 mai 1995 Gaz. Pal. 1995 . II . chron. 457 note Doucet
[9] " Pédophilie incontrôlable sur le Net " Libération 30 août 1996 – " Les vices cachés d'Internet " Le Figaro 19 août 1996
[10] autres forums, cités par Raffi Garo Haladjian,Gérant de FranceNet " Comment devenir pédophile en 24 heures.. " http://www.francenet.fr/comment/comment.html : "alt.binaries.pictures.erotica.child.female", "alt.binaries.pictures.erotica.child.male","alt.binaries.pictures.erotica.children","alt.binaries.pictures.erotica.lolita","alt.binaries.pictures.erotica.pre-teen", "alt.binaries.pictures.erotica.schoolgirl", "alt.sex.pre-teens", "alt.binaries.pictures.lolita.fucking", "alt.binaries.pictures.lolita.misc", "alt.sex.stories.incest"
[11] " Pornography on Internet " Yaman Akdeniz http://www.argia.fr/lij
[12] voir le Rapport du MAPI (partie 2) http://www.info.fundp.ac.be/~~mapi/mapi-fr.html
[13] 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

mineur, sauf s'il est établi que cette personne était âgée de 18 ans au jour de la fixation ou de l'enregistrement de son image. ".
Désormais, les personnes morales peuvent être poursuivies en tant qu'auteurs de cette infraction (art. 227-28-1 CP).

Cinq modifications majeures ont été apportées à cette incrimination.
Tout d'abord, le Sénat[14] a proposé l'ajout à côté du terme d'" image " de celui de " représentation " afin de viser les images virtuelles qui peuvent également représenter, et ce de façon réaliste, un mineur. Il a de plus aggravé les peines privatives de liberté en prévoyant une sanction de 3 ans d'emprisonnement et de 5 ans en cas de circonstance aggravante. Toujours en ce qui concerne la sanction, l'art. 227-31 CP introduit par la loi de juin 1998 permet à la juridiction de jugement de prononcer à titre complémentaire à une peine d'emprisonnement assortie d'un sursis avec mise à l'épreuve, ou à titre principal, un suivi socio-judiciaire. Ce dernier peut avoir une durée de 10 ans et comprendre une injonction de soins[15]. Quant à l'Assemblée Nationale, elle est à l'origine de l'introduction d'une présomption simple de minorité des personnes dont l'image est diffusée. Les députés ont également voté la suppression de la circonstance aggravante fondée sur l'âge du mineur qui existait dans la rédaction originelle de l'incrimination et la création de la circonstance aggravante d'utilisation d'un réseau de télécommunications pour diffuser ces images. Cette disposition confirme ainsi que le champ d'application de l'art. 227-23 CP inclue les images pornographiques de mineur diffusées sur Internet et souligne le caractère hautement répréhensible de ce comportement. Il faut d'ailleurs ajouter que la loi du 17 juin 1998 fait de l'usage d'un réseau de télécommunications une circonstance aggravante de certaines infractions sexuelles lorsqu'il en a facilité la mise en contact entre l'auteur et la victime[16].

Enfin, on peut noter que la député Mme Boutin a proposé un amendement qui avait pour but de remplacer dans la formulation de la circonstance aggravante l'expression " *à destination d'un public non-déterminé* " par celle "*à destination du public* ". Les députés ne l'ont pas retenu car la Commission et le Gouvernement n'en ont pas compris le sens. Mais l'argument avancé par Mme Boutin n'était pas dépourvu d'intérêt. Elle craignait que l'expression " *un public non-déterminé* " ne garantisse à certains responsables de serveurs une impunité. En effet, si une image pornographique de mineur est diffusée sur un forum, la circonstance aggravante pourra s'appliquer, le forum pouvant constituer un public non-déterminé. Mais si la même image est diffusée sur un forum dont l'accès est contrôlé, ou par courrier électronique grâce à des *mailing lists* ; les responsables pourront arguer du fait que le public auquel est destiné ces images est tout à fait déterminé, puisque recensé sur une liste. Il est sans doute regrettable que cet amendement ait été rejeté.

En ce qui concerne la procédure, la loi de juin 1998 facilite les poursuites. En principe, la loi pénale française n'est applicable à l'encontre d'un Français ou d'une personne résidant habituellement en France ayant commis une infraction à l'étranger, qu'en cas de réciprocité de l'incrimination et du dépôt préalable d'une plainte par la victime, ses ayants droits ou les autorités du pays où les faits ont été commis. Désormais, les poursuites pour diffusion d'images pornographiques de mineurs dans cette hypothèse ne sont plus soumises aux conditions énoncées (art. 227-27-1 CP). La loi incite même indirectement aux poursuites en exigeant la motivation et la notification de l'avis de classement sans suite (al. 1er art. 40 CPP). Enfin, les empreintes génétiques des personnes condamnées pour cette infraction pourront (ou devront ?) figurer dans le fichier des traces génétique prévu par le nouvel article 706-54 CPP.

B. LES PROVOCATIONS AU SENS LARGE

Lorsqu'on diffuse un message, il se peut que seules quelques personnes se sentent concernées. Grâce à Internet, l'auditoire de chaque message est décuplé, ainsi que le nombre de personnes interpellées par l'information. Cette diffusion à grande échelle constitue un atout aussi bien pour les entreprises qui souhaitent présenter leurs produits à une nouvelle clientèle (I) que pour ceux qui veulent répandre des idées contestables (II & III).

I. LA PUBLICITE

Depuis 1995, la publicité a connu un essor phénoménal sur Internet : en 1997, le marché avait explosé en un an de 300 % aux Etats-Unis[17]. Il représenterait 850 millions de dollars (toujours aux Etats-Unis).

[14] projet de loi J.O.AN 30 oct 1997
[15] C'est pourquoi le nouvel art. 706-47 CPP prévoit l'expertise médicale du prévenu avant tout jugement sur le fond.
[16] ces infractions sont : le viol (art. 222-24), les agressions sexuelles (art. 222-28), le proxénétisme (art. 225-7), la corruption de mineur (art. 227-22), l'atteinte sexuelle dur mineur de 15 ans (art. 227-26)
[17] " Des bannières par milliers " e-Links n°3 nov. 1997

Cette attraction des annonceurs pour ce type de support publicitaire s'explique notamment son caractère interactif : la publicité se présente sous la forme d'une bannière sur laquelle l'internaute peut cliquer pour obtenir de plus amples renseignements sur le produit vanté. La présence d'Internet est également fondamentale pour les internautes puisqu'elle sponsorise certains sites qui ne pourraient pas exister sans elle. Mais la publicité peut également s'exprimer dans le contenu d'un site, de façon plus ou moins explicite et là commence le danger.
Or, la législation française réglemente la publicité et ce façon générale et particulière.

Les dispositions de l'art. 44 de la loi du 27 décembre 1993 s'appliquent à toute publicité. Elles interdisent la **publicité mensongère** qui se définit comme celle " *qui comporte des allégations, indications, ou présentation fausses ou de nature à induire en erreur* ". Elle est alors sanctionnée par 2 ans d'emprisonnement et 250 000 F d'amende à l'encontre de l'annonceur. La loi ajoute que le responsable du support est complice dès lors que les conditions de droit commun de la responsabilité sont réunies : si le message est visiblement excessif, le responsable du support doit demander des justifications de la véracité des affirmations faute de quoi il engagera sa responsabilité.
De nombreux autres pays interdisent ce type de publicité (parfois par la loi civile uniquement). Il existe d'ailleurs une directive communautaire du 10 septembre 1984 relative au rapprochement des législations dans le domaine de la publicité trompeuse.

De plus, l'art. 2 de la loi n°97-665 du 4 août 1994, dite loi Toubon, impose que toute offre de produits ou de services ainsi que toute publicité écrite, ou parlée, ou audiovisuelle soit faite **en langue française**. Le manquement à ces dispositions constitue une contravention de la 4ème classe.

Certaines publicités relatives à certains produits sont encadrées par la loi, soit qu'elle les interdisent ou les soumettent à des conditions particulières. C'est le cas de la publicité pour les boissons alcooliques[18], pour le tabac[19], pour les médicaments[20], en faveur des armes à feu[21], pour les produits, objets et méthodes pour se suicider[22].

II. LA PROVOCATION STRICTO SENSU

Internet peut être le vecteur de toute sorte de provocations, quelles soient publiques (comme en matière de publicité) ou privées. Les propos constitutifs de provocation les plus répandues sont les propos racistes, de négation des crimes contre l'Humanité[23] commis durant la IInde Guerre mondiale ou présentant les drogues sous un jour favorable.

Certaines sont réprimées en droit français quand elles ont simplement été formulées[24], d'autres lorsqu'elles ont été suivies d'effet. Par cette formule d' " effet ", on entend que la " victime " de la provocation

[18] Les art. L.17 à L.20 du Code des Débits de Boissons prévoient les indications qui peuvent et doivent figurer sur la publicité. De plus, l'art. L. 17 précise quels sont les modes de diffusion exclusivement autorisés. Evidemment Internet n'est pas visé et seuls trois types de supports pourraient s'en rapprocher. Il s'agit de la presse écrite, de la radiodiffusion sonore (mais dans les conditions déterminées par le Conseil d'Etat), l'envoi de circulaires commerciales. Si le courrier électronique peut être assimilé à la troisième catégorie, les sites qui diffusent des publicités ne sont certainement pas assimilables à la presse écrite, à la radio. Au contraire, si l'on continue à considérer que le web est un service de communication audiovisuelle, la publicité pour les alcools devrait y être prohibée. Selon l'art. L.21, le manquement à ces dispositions fait encourir une amende de 500 000 F.

[19] l'al. 1er de l'art. L.335-24 du Code de la Santé publique énonce que " toute propagande ou publicité, directe ou indirecte, en faveur du tabac ou des produits du tabac .. sont interdits "

[20] Si certains médicaments peuvent faire l'objet de publicité après délivrance d'un visa du Ministère de la Santé et consultation d'une Commission spécialisée, la publicité d'autres médicaments ou " produits, objets, appareils et méthodes présentés comme favorisant le diagnostic, la prévention ou le traitement des maladies " est strictement interdite par le Code de la Santé Publique. La sanction est une amende de 20 000 F et en cas de récidive de 200 000 F (" La publicité pour les médicaments " M.V. Jeannin Gaz.Pal. 1993.I.p.657

[21] art. 6 L.12 juil 1985 sanctionne les manquements aux dispositions d'une amende de 300 000 F

[22] art. 223-14 CP sanctionne toute publicité pour ces produits de 3 ans d'emprisonnement et 300 000 F d'amende

[23] Pour s'en rendre compte par soi-même : http://www.abbc.com/aaargh/ - http://abbc.com/islam/french/textes/

[24] à l'usage illicite de stupéfiant à l'encontre d'un mineur (art. 227-18), à l'usage de stupéfiant (art. L.630 CSP), à la consommation d'alcool à l'encontre d'un mineur (art. 227-19 CP), à la mendicité à l'encontre d'un mineur (art. 227-20 CP), à la commission de crimes ou de délits à l'encontre d'un mineur (art. 227-21 CP, à la commission de certaines infractions (art. 24 L. 29 juill 1881), non publique à la discrimination raciale, religieuse.. (art. R. 625-7 CP), à des rassemblements d'insurgés (art. 412-4 CP), à s'armer contre l'autorité de l'Etat (art. 412-8 CP), à l'encontre des militaires à passer au service d'une puissance étrangère (art. 413-1 CP), à l'encontre des militaires à la désobéissance (art. 413-3 CP), à la démoralisation de l'armée (art. 413-4 CP), à un attroupement armé (art. 431-6 CP), à la rébellion (art. 433-10 CP)

aura commis l'acte auquel on l'incite ou aura au moins tenté de le commettre. Cela signifie donc que la juridiction qui aura à statuer sur la provocation ne pourra le faire qu'après que l'on a statué sur la réalité de l'acte ou de sa tentative. Il faut de plus noter que cet effet sera parfois exigé pour que la provocation soit constituée[25], tandis qu'il ne constituera qu'une circonstance aggravante dans d'autres hypothèses[26]. Il faut ajouter que la loi du 17 juin 1998[27] prévoit la responsabilité pénales des personnes morales dans le cadre de certaines provocations.

III. L'APOLOGIE

Selon la jurisprudence[28], l'apologie est une infraction distincte de la provocation. Mais elle s'en rapproche car elle se veut incitative à l'égard de celui qui la perçoit.
La loi du 29 juillet 1881 sanctionne toute apologie des atteintes volontaires à la vie, à l'intégrité des personnes, des agressions sexuelles, des actes de terrorisme, des crimes de guerres, des crimes contre l'Humanité, des crimes ou délits de collaboration avec l'ennemi.
S'en rapproche la contestation des crimes contre l'Humanité incriminée par l'art. 24bis.

C. LA REVELATION D'UN SECRET

Nous avons choisi d'étudier les atteintes au secret dans ce paragraphe consacré aux atteintes à la société, car bien que certaines violations de secret portent plus atteinte à un individu qu'à la société, d'autres portent atteinte à cette dernière également. De plus, le secret une règle établie par la société selon laquelle tout individu, dans certains contextes, doit pouvoir divulguer certaines informations en toute confiance.

Ainsi, le Code pénal sanctionne toute violation du ***secret de la défense nationale*** par ses articles 413-10 et 413-11.

La révélation d'un ***secret professionnel*** est également sanctionnée pénalement par l'art. 226-13 CP. Le ***secret de l'instruction***, énoncé par l'art. 11 CPP, est ainsi protégé en tant que secret professionnel par l'art. 226-13. L'une des premières affaires liées à Internet portait d'ailleurs sur la violation de ce secret : mécontent d'une détention provisoire jugée arbitraire, C. Proust avait communiquer sur Internet le dossier d'instruction de l'affaire Gigastorage[29]. De même, aux Etats-Unis, où les dépositions des témoins sont également secrètes, le père d'un enfant paralysé à la suite d'une agression à l'école a affiché sur le web les pièces du dossier du procès[30].

De plus, ***le secret des correspondances*** est protégé par les dispositions pénales de l'art. 226-15 CP. Cet article permet de poursuivre la diffusion sur Internet de correspondances quelque soit leur nature : lettres, communications téléphoniques ou communications transmises par Internet[31]. En effet, l'alinéa 2 incrimine " *le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ".

§2. LA PROTECTION DES INDIVIDUS

Certaines informations circulant sur le réseau peuvent porter atteinte au droit de propriété des personnes (A.), à leur personnalité (B.) ou à leur intégrité psychique (C.).

A. LES ATTEINTES A LA PROPRIETE

[25] au suicide (art. 223-13 CP), à la commission de crimes et délits quels qu'ils soient (art. 23 L. 29 juill . 1881), à la tentative de commission d'espionnage et de trahison (art. 411-11 CP)
[26] à s'armer contre l'autorité de l'Etat (art. 412-8 CP), à un attroupement armé (art. 431-6 CP)
[27] 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
[28] Crim. 11 juill. 1972 Bull. Crim. n°236
[29] voir *Les autoroutes de l'information* C. Bernat coll. Travaux de Recherche Panthéon-Assas Paris II éd. L.G.D.J. 1997 p. 85
[30] Le Monde 29 janvier 1998
[31] un exemple : en septembre 1997, les messages émis sur un récepteur de poche du service de sécurité du Président des Etats-Unis s'affichaient automatiquement sur un site web - " La cyber-flibuste, vent en poupe " Le Figaro 5 déc. 1997

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 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. Notre droit est donc doué d'une faculté d'adaptation qui le place d'emblée au premier rang des lois applicables à Internet.* "[32] Celle-ci peut concerner le nom d'une marque (I.) ou une œuvre de l'esprit (II.).

I. LA CONTREFAÇON D'UNE MARQUE

De nombreuses affaires de conflits relatifs au nom de domaine ont vu le jour[33]. Elles opposent les titulaires de nom de domaine aux titulaires de droits de propriété industrielle sous forme de marques déposées, qui se voient refuser un nom de domaine sur Internet identique à leur marque. Certains même se spécialisent dans le commerce de nom : ils déposent des noms d'adresse empruntant le nom d'une marque prestigieuse pour la lui revendre ensuite.

II. LA CONTREFAÇON D'UNE ŒUVRE DE L'ESPRIT

Celle-ci peut être constituée par la diffusion sur le réseau de toute œuvre de l'esprit pouvant circuler sur un support multimédia comme Internet : un livre, un article, une musique, un logiciel, un film…Les exemples sont déjà nombreux, le plus célèbre en France étant celui du gérant d'un cybercafé de Besançon, qui avait en janvier 1996 scannérisé le livre " Le grand secret " du Dr. Gübler pour ensuite le diffuser sur son site web (depuis, de nombreux sites l'ont reproduit). Il existe de nombreux sites qui diffusent des chansons ainsi que leurs paroles et partitions, sans l'autorisation de leurs auteurs[34]. De nombreuses affaires de contrefaçon ont également été soulevées par des journalistes dont les articles ou les reportages ont été diffusés sans leur consentement sur Internet[35], comme celle de la société SDV Plurimédia qui diffusait des reportages provenant des " Dernières nouvelles d'Alsace " et de France 3 Alsace.
Il semble que la contrefaçon puisse être également constituée lorsqu'un serveur crée un lien hypertexte avec un autre site sans son autorisation et que ce lien donne l'apparence de découvrir une nouvelle page du premier site et non celle d'un autre site.

Ces litiges relèvent de l'application des dispositions du Code de la Propriété Intellectuelle et plus précisément de l'art.L.335-3. Ce dernier incrimine le fait de reproduire, représenter ou diffuser une œuvre de l'esprit en méconnaissant les droits de l'auteur sur cette œuvre, c'est-à-dire sans son consentement (art.L.122-4). La difficulté relative à Internet est de déterminer si diffuser sur le réseau, par quelque service que ce soit, l'œuvre d'autrui constitue bien une reproduction, ou une représentation.
La reproduction se définit (art. L.122-3 CPI) comme " *la fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte* ". Toutefois, l'art. L.122-5 CPI autorise les copies privées qui doivent comme leur nom l'indique, ne pas être destinées à une utilisation collective, et les courtes citations dès lors qu'est indiqué le nom de l'auteur et la source et qu'elles soient " *justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées* ". Quant à la représentation, elle consiste selon l'art. 122-1 CPI dans " *la communication de l'œuvre au public par un procédé quelconque, et notamment, par récitation publique, exécution lyrique../..par télédiffusion* ".
Nous verrons que le jurisprudence considère déjà que mettre en ligne sur un site web une œuvre constitue une reproduction et une représentation. Par contre, on peut se demander si ces notions sont applicables au courrier électronique.

B. LES ATTEINTES A LA PERSONNALITE

[32] " Prévenir les atteintes à la propriété littéraire et artistique sur Internet " http://www.celog.fr/expertises
[33] " Au fil du Net " Gaz. Pal. 23,24 juill 1997 p. 9
[34] Pour un exemple relatif de sites diffusant des contrefaçons de J.M. Jarre – Expertises n°210 déc. 1997 p. 367
[35] Trib. 1ère instance de Bruxelle 16 oct 1996 : Agjip, SAJ, Sofam et 21 journalistes c/ Central Station – Ord. Réf. TGI Strasbourg 3 fév. 1998 SNJ, CFDT c/ SDV Plurimédia (JCP1998.II.10044)

I. LE DROIT A L'IMAGE, LE DROIT A LA VOIX

Ce droit est assez proche du droit de l'auteur d'une œuvre : l'image, la voix se rapprochent des œuvres. Il se peut qu'un internaute diffuse sur le réseau l'image d'un individu ou ses propos, sans le consentement de celui-ci. Il n'est pas admissible de rendre accessible à tout à chacun la création d'une personne, alors encore moins l'un des attributs de sa personnalité[36].

Dans cette hypothèse, les articles 226-2 et 226-8 CP peuvent être appliqués à Internet grâce au large champ d'application que leur permet leur formulation. Effectivement, ces deux articles visent une " diffusion " faite " *de quelque manière que ce soit* " (art. 226-2) ou " *par quelque voie que ce soit* ". De plus, ces deux dispositions prévoient, le cas échéant, l'application des règles particulières relative à la détermination des personnes responsables en matière de presse et d'audiovisuel. Nous pouvons ajouter que la Chambre Criminelle a récemment considéré que le délit de l'art. 226-2 était un délit continu[37] (on peut dès lors se demander si celui de l'art. 226-8 ne doit pas l'être aussi).

Il n'existe que trois conditions : . La première relève de la procédure : l'art. 226-6 exige pour toute poursuite que la victime ait déposé plainte. La seconde est commune aux deux hypothèses et est que l'auteur agisse sans le consentement de l'intéressé. Il est évident que la diffusion en direct sur Internet de la vie quotidienne d'une étudiante américaine bien connue des internautes ne relèverait pas de ces dispositions puisqu'elle a donné son accord. La dernière relève de la nature du document : il est nécessaire pour qu'il y ait infraction soit que le document ait été enregistré dans des circonstances attentatoires à la vie privée, soit que le document constitue un montage. Deux situations sont donc à distinguer.

1. L'image ou l'enregistrement obtenu dans des circonstances privées

L'art. 226-2 CP s'applique aux **documents** visés par l'art. 226-1. Ils se caractérisent par deux conditions.

- Il doit s'agir :
  → Soit de paroles prononcées à titre privé ou confidentiel, qui ont été captées, enregistrées ou transmises par un procédé quelconque.
  Il n'est plus exigé comme dans l'art. 368 de l'ancien Code Pénal qu'elles aient été prononcées dans un lieu privé ; il suffit qu'elles aient prononcées, même dans un lieu public, à titre privé ou confidentiel. Il peut donc s'agir aussi bien de paroles échangées dans la rue, à un domicile, au bureau, qu'au téléphone ou que sur un service vocal d'Internet.
  → Soit de l'image d'une personne se trouvant dans un lieu privé, qui a été fixée, enregistrée ou transmise par un procédé quelconque.
  La remarque relative aux paroles est transposable à l'image : cette dernière peut avoir été fixée dans tout lieu privé, y compris un service visuel d'Internet qui aurait le caractère privé.
  Si les images ou les paroles n'ont pas le caractère privé exigé par la loi, aucune sanction ne peut être prise et reste l'action civile sur la base de l'art.9 CCiv.
- L'art. 226-1 ajoute de plus que ces documents doivent être obtenus " *volontairement* ", dans le but de " *porter atteinte à l'intimité de la vie privée* ". On peut penser que cette condition est exigée par l'art. 226-2 : Il faudrait que le document diffusé ait été obtenu avec cette intention particulière. Mais nous allons voir que cette exigence peut restreindre le champ d'application de l'art.226-2.

Le **comportement** sanctionné est le fait de " *conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser*" ces documents.
L'avantage de cette formulation est qu'elle permettra, si le cas se présente, d'écarter toute argumentation fondée sur le fait que dans le World Wide Web, ce ne sont pas les sites qui diffusent leur contenu, mais les utilisateurs qui viennent chercher l'information[38]. Que l'on adopte l'une ou l'autre des conceptions, l'article trouvera à s'appliquer du fait de l'expression " porter ou laisser porter " qui vise aussi bien un acte positif d'émission qu'un acte négatif, ainsi que l'existence de destinataires singulier (le tiers) et pluriel (le public).

De plus, nous pouvons relever que ces dispositions répriment également le recel des documents visés dans la mesure où le fait de les conserver est également incriminé.

---

[36] " La protection des droits de la personnalité sur les réseaux multimédia " E. Pierrat http://www.grolier.fr/cyberlex.net
[37] Crim. 4 mars 1997 Bull. Crim. n°83
[38] conception soutenue par le défendeur dans l'affaire Art Music France c/ Ecole Nationale Supérieure des Télécommunications TGI Paris Ord . Réf. 14 août 1996 – D. 1997 Jur. P.490

Quant à **l'élément moral** de celui qui diffuse les documents, aucune intention particulière de porter atteinte à la vie privée n'est exigée comme dans l'art. 226-1. Nous avons dit que par contre cette intention semblait nécessaire lors de l'enregistrement des paroles ou de la fixation de l'image, étant entendu que l'auteur des enregistrements ou documents peut ne pas être le même que celui de leur diffusion. Faut-il exiger cette intention lors de l'obtention du document ?
Ne pas l'exiger revient à sanctionner celui qui diffuse le document même si ce dernier n'a pas été obtenu avec l'intention de porter atteinte à la vie privée de la personne concernée. Cela permettrait de poursuivre des éditeurs peu scrupuleux (sur Internet ou dans la presse traditionnelle) qui publieraient par exemple des photos de famille pour lesquelles une personnalité aurait posé, mais destinées au cercle familial. Cette conception, bien qu'utile en matière de presse à scandale, serait contraire au principe d'interprétation stricte de la loi pénale et n'est pas retenue[39].

Les sanctions sont les mêmes que celles prévues par l'art. 226-1, c'est-à-dire un an d'emprisonnement et 300 000 F d'amende pour les personnes physiques et une amende de 1 500 000 F pour les personnes morales. Ces dernières peuvent de plus être condamnées à une interdiction d'exercer l'activité professionnelle dans l'exercice de laquelle l'infraction a été commise. Les deux types de personnes peuvent être condamnés à l'affichage ou la diffusion de la décision de justice (art. 226-7 pour les personnes morales et art. 226-31 pour les personnes physiques).

2. L'image ou l'enregistrement utilisé pour un montage

L'art. 226-8 CP punit de un an d'emprisonnement et de 100 000 F d'amende la personne physique et de 500 000 F la personne physique qui publie " *par quelque voie que ce soit, le montage réalisé avec les paroles et images 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* ".
Cette incrimination mérite quatre remarques.

- Contrairement à celle de l'art. 226-2, les documents utilisés n'ont pas à porter atteinte à la vie privée, ce qui permet d'incriminer des montages faits avec des photos ou paroles officielles.
- La constitution de l'infraction nécessite qu'il y ait un **montage**. Il faut indiquer que la Cour d'appel de Toulouse a considéré dans un arrêt du 26 février 1974[40] que " *le montage ne constitue pas nécessairement une manipulation ou un trucage de la photographie, mais se trouve réalisé dès lors que l'insertion de cette photographie dans un contexte d'images, de dessins ou de légendes en modifie la valeur artistique, la portée ou la signification* ". Pour prendre un exemple, cela signifie que diffuser sur un site consacré à la chasse, la représentation, sans trucages mais permettant tout type d'interprétation , d'un défenseur de la cause animale peut constituer un montage dès lors qu'elle laisse penser que cette personne est favorable à la chasse. Dès lors, dans certaines hypothèses, il y aura du fait de cette interprétation du montage, cumul de qualifications.
- L'infraction n'est pas constituée lorsqu'il apparaît à l'**évidence** qu'il s'agit d'un montage ou qu'il en est fait **expressément mention**. Si la mention ne pose aucune difficulté puisqu'elle doit être expresse, on peut par contre se demander comment doit être appréciée l'évidence du montage. Il est évident qu'elle peut être appréciée par rapport à ce que l'on voit ou ce que l'on entend, c'est-à-dire par rapport aux défauts de la technique de montage. Mais peut-elle être appréciée par rapport à ce que l'on sait ? La réponse est a priori positive. Ainsi, l'infraction sera sans doute constituée si un serveur diffusait une image parfaitement truquée du Président de la République en voyage sur la Lune car il est évident qu'il ne peut s'agir que d'un montage. Mais cette évidence par rapport à ce que l'on sait est sans doute difficile à apprécier dans la mesure elle nécessite une appréciation in concreto.
- L'art. 226-8 CP vise le fait de publier. Ce comportement doit s'entendre au sens de " rendre publique ", même de façon restreinte[41]. Les difficultés déjà évoquées relatives au comportement passif ou actif de l'éditeur de contenu d'un site pourraient ici être soulevées. Mais on pourrait considérer par analogie avec l'art. 226-2 que la publicité s'entende du fait de porter ou de laisser porter à la connaissance du public ou d'un tiers le montage.

II. LES INFORMATIONS NOMINATIVES[42]

[39] *Droit pénal spécial* M. Véron coll. U éd. Masson/Armand Colin 1996
[40] D. 1974. 736 – Rev. Sc. Crim. 1976. 119
[41] Crim. 30 janv. 1978 – Bull. Crim.n°34
[42] *Données personnelles et société de l'information* – G. Braibant – Documentation française coll. des Rapports Officiels

Sur Internet, on peut communiquer des informations nominatives, qu'elles aient été recueillies régulièrement en dehors d'Internet ou sur le réseau. Or celles-ci font l'objet d'une protection organisée par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui a été prise pour encadrer le développement de l'informatique afin que celle-ci ne porte atteinte " *ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* " (art. 1er).

Pour pouvoir communiquer ces informations, il faut respecter certaines dispositions sanctionnées pénalement. Celui qui divulguerait sur Internet ce type d'informations sans les respecter, pourrait être poursuivi.

Le danger de ces bases de données personnelles est grand ; bien plus grand qu'auparavant car désormais, ces bases de données sont beaucoup plus facilement accessibles et peuvent se recouper avec d'autres, ce qui permet de connaître tous les aspects de la vie privée d'une personne[43]

1. Définition des données nominatives

Selon l'art. 4 L. 6 janv. 1978, les données nominatives sont " *les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent* ".

La difficulté avec Internet est que ce mode de communication permet l'exploitation du multimédia. Or, ce support d'informations n'avait pas été prévu par la loi de 1978.

La CNIL a considéré que l'image pouvait constituer une information nominative à l'occasion d'une recommandation relative aux dispositifs de vidéosurveillance[44]. Par contre, le gouvernement a considéré qu'une image seule ne peut constituer une information nominative.

La transposition des directives du 24 octobre 1995[45] et du 15 décembre 1997[46] (qui devra avoir lieu avant la fin de 1998) devrait résoudre cette question puisqu'elle étend la protection au multimédia, c'est à dire à toutes les informations nominatives sous formes de texte, d'images ou de sons[47].

2. Les comportements pénalement sanctionnés

a) *Ne pas respecter les règles de constitution du traitement*

Le traitement se définit selon la directive comme " *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* " (voir aussi art. 5 L.6 janv. 1978).

Jusqu'à présent, on distingue deux types de règles de constitution :Si le traitement est crée dans le cadre d'un établissement privé, on doit faire une déclaration préalable. S'il l'est dans le cadre d'un établissement public, la constitution du traitement nécessite un avis préalable de la CNIL, auquel on ne peut passer outre que par un décret (pris sur avis conforme du Conseil d'Etat)[48].

---

[43] " Vie privée à vendre sur le réseau " Le Monde cahiers multimédia 15, 16 juin 1997

[44] 1994 – " *par leurs caractéristiques, notamment grâce à l'amélioration de la définition des images, à la capacité de stockage de données et à la diffusion de logiciels de manipulation de fichiers résultant de la transformation de ces images en données numérisées susceptibles d'êtres traitées en ordinateur, comme peut l'être un fichier de caractères alphanumériques issus d'un texte, ces applications ainsi modernisées seront, à la fois, et plus efficaces, et plus dangereuses pour les libertés individuelles* ".

[45] Directive 95/46/CE du Parlement européen et du Conseil du 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données – JOCE 23 nov. 1995, n°L.281 p.31

[46] Directive 97/66/CE du Parlement européen et du Conseil du 15 déc 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications– JOCE30 janv. 1998, n°L.24 p.1

[47] " L'union européenne et la protection des données " P. Bischoff Rev. Du Marché commun et de l'Union européenne n°421 sept 1998 p. 537

[48] Excepté dans le cadre de normes simplifiées ou des fichiers de santé pour les quels l'avis d'un comité spécialisé est nécessaire.

En matière de traitement proposé sur Internet, la CNIL a eu l'occasion d'énoncer des règles qu'il convient de respecter pour obtenir un avis favorable.
La CNIL était saisie de deux demandes de constitution d'annuaires sur Internet[49]. La commission a rendu un avis favorable car le traitement :

- A une finalité légitime et pertinente (" *favoriser les communications et les échanges entre les chercheurs du monde entier* ")
- Porte sur des informations limitées (le sexe, le nom, les prénoms, le lieu de travail et le service d'affectation, les numéros de téléphone, de télécopie et l'adresse " courrier électronique " professionnels, les mots-clés caractérisant l'emploi occupé, un lien hypertexte pour accéder aux publications scientifiques du chercheur publiées sur le réseau)
- Exige l'accord des personnes recensées, accord qui pourra à tout moment être révoqué
- Fera apparaître un avis rappelant les droits, garanties et protections dont bénéficient les personnes recensées (de plus, un lien hypertexte pourra renvoyer à une page diffusant le texte de la loi du 6 janvier 1978)

Dans une recommandation du 8 juillet 1997[50], la CNIL ajoute que les personnes recensées dans un annuaire en ligne doivent être " *clairement et préalablement informées par les éditeurs d'annuaires sur Internet des risques inhérents* (captation, falsification, détournement de la finalité) *à la diffusion sur un réseau international ouvert des données les concernant* ".

De plus l'art. 31 L.1978 précise que la mise en mémoire des données nominatives " *qui directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs de la personnes* " est interdite sauf accord exprès de l'intéressé ou que les utilisateurs de ces traitements soient des églises, des mouvements à caractère religieux, philosophique, politique ou syndical.

Ces régimes de déclaration et d'autorisations seront modifiés lorsque la directive sera transposée en droit interne. La directive prévoit comme principe une absence de contrôle a priori des traitement et n'exige qu'une déclaration préalable (dans certaines hypothèses, cette déclaration est même écartée).

Le contrôle a priori est uniquement requis lorsque le traitement est " *susceptible de présenter des risques particulier au regard des droits et libertés des personnes concernées* ". Selon le considérant 53, l'appréciation de ces " traitements à risque " est laissée aux Etats, mais la directive donne des pistes : il s'agirait de risques attenant à la nature, à la portée ou aux finalités du traitement. La CNIL a déjà dégagé 10 catégories de traitement qui doivent être considérés à risques[51].

En ce qui concerne les sanctions encourues en cas de non respect de ses dispositions, l'art. 226-16 CP sanctionne de 3 ans d'emprisonnement et de 300 000 F d'amende le fait de constituer ou de faire constituer un traitement sans respecter les formalités précitées, que cette omission soit volontaire ou non.

L'art. 226-19 CP sanctionne quant à lui le fait mettre ou de conserver en mémoire informatisée des données nominatives qui directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs de la personnes, ainsi que les informations nominatives concernant des infractions, des condamnations ou des mesures de sûreté. La peine de cette infraction est lourde car il s'agit de 5 ans d'emprisonnement et de 2 000 000 F d'amende.

b) Ne pas respecter les règles de divulgation

Ces traitements sont autorisés dans la mesure où leur finalité est considérée comme légitime. Souvent, cela implique que les informations ne seront communiquées qu'à un nombre limité de personnes dans le cadre d'une activité particulière.

C'est pourquoi l'art. 226-22 réprime le fait pour celui qui a recueilli les informations durant leur traitement, de divulguer ces informations à des tiers (qui n'a pas qualité pour les recevoir) sans l'autorisation de l'intéressé lorsque leur divulgation " *aurait pour effet de porter atteinte à la considération de l'intéressé, ou à l'intimité de sa vie privée* ". Lorsque cette divulgation est volontaire, son auteur encourt 1 an d'emprisonnement et 100 000 F d'amende et lorsqu'elle est involontaire, 50 000 F d'amende.

---

[49] Délibérations de la CNIL n°95-131 & 95-132 - 7 nov. 1995 : Centre national de calcul parallèle des sciences de la terre et Institut de physique nucléaire d'Orsay – Gaz. Pal. 1996 n°26, 27 p.36
[50] Délibération de la CNIL n°97-060 8 juillet 1997-J.O. 2 août 1997 p. 11517 - " Au fil du Net " Gaz. Pal. 7, 9 déc. 1997
[51] 17ème rapport d'activité de la CNIL pour 1996 p.28

Ainsi, nous pouvons nous demander si les sites que certains Etats américains proposent, sur lesquels on peut vérifier que son voisin n'a pas été condamné pour avoir commis une infraction sexuelle[52] (au demeurant autorisés par la loi Megan) pourraient être créés en France, sans l'intervention d'une loi. A n'en pas douter, les condamnations judiciaires constituent une information dont la divulgation pourrait avoir comme effet de porter atteinte à la considération du condamné. C'est d'ailleurs la raison pour laquelle l'art. 226-19 CP en sanctionne la mise en mémoire sans l'accord de l'intéressé ou sans l'autorisation de la loi. La Chambre Criminelle[53] vient de plus de considérer que la prescription de l'action publique contre cette infraction, du fait de son caractère clandestin, ne commence à courir que lorsqu'elle a été constatée en tous ses éléments et que l'atteinte portée aux droits des victimes soit révélée à ces dernières.

L'incrimination de l'art. 226-22 CP vise le fait de divulguer des informations dont la divulgation pourrait avoir pour effet de porter atteinte à la considération ou à l'intimité, que cet acte soit volontaire ou non. Lorsque cet acte est volontaire, l'élément moral est de savoir que la divulgation entraînera peut-être une atteinte à la considération ou à l'intimité de la personne, mais ce n'est pas la volonté de porter par cet acte l'atteinte. On peut penser si cette volonté, bien plus grave que celle réprimée par l'art. 226-22, motivait celui qui divulgue les informations nominatives à un tiers, on pourrait appliquer l'art.226-21 qui sanctionne le fait de détourner les informations de la finalité du traitement. Divulguer les informations pour nuire, c'est détourner la finalité. La sanction serait alors bien plus lourde : 5 ans d'emprisonnement et 2 000 000 F d'amende.

c) *La difficulté des flux de données transfrontières*

Du fait du caractère international d'Internet, les données peuvent être traitées en France, puis communiquées à l'étranger et inversement. De ce fait, on peut craindre que les garanties apportées par la loi de 1978 ne soient pas respectées.
Selon P. Huet[54], on doit appliquer la législation (donc quand elle existe) du pays dans lequel les données seront traitées. Ainsi, si les données sont traitées en France, puis envoyées à l'étranger, on doit respecter la législation française (comme cela a été fait pour les annuaires). Par contre, les données traitées à l'étranger, puis communiquées en France relève de la loi étrangère. Pour limiter les conséquences néfastes de flux de données dans des pays n'offrant pas ou peu de protection, la directive du 24 octobre 1995[55] permet de refuser le transfert des données lorsque le pays est tiers à l'Union et qu'il ne garantie pas une " protection adéquate " des données (dont l'appréciation est faite par la Commission).

III. *LA DIFFAMATION, L'INJURE, LA DENONCIATION CALOMNIEUSE*

Il est très facile de mener une campagne de dénigrement grâce à Internet. Les mésaventures du 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[56].

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[57]. 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* ".

---

[52] site de l'Etat de Floride http://www.fdle.state.fl.us/
[53] Crim. 4 mars 1997 Bull. Crim. n°83
[54] *Le droit du multimédia* éd. du téléphone 1996 AFTEL sous la direction de P. Huet
[55] la Convention du Conseil de l'Europe 108 de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel avait également pris des dispositions permettant aux Etats de refuser le flux si la législation du pays destinataire n'apportait pas de protection équivalente.
[56] " 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
[57] *Guerres dans le cyberespace* J. Guisnel 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[58].

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 a protéger les personnes morales[59], dès lors que l'attaque ne se constitue pas de dénigrement des produits, des services ou des prestations offerts par la personne morale[60].
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 CP.

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[61].

C. LES ATTEINTES A L'INTEGRITE 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[62].

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 (un crime ou un délit) ou sur la commission d'une infraction contre les biens (une destruction, dégradation ou détérioration d'un bien), et selon que la menace est simple ou émise sous condition. Nous les étudierons sous l'angle de la dernière distinction.

Les menaces simples

Lorsqu'elles portent sur la commission d'un crime ou d'un délit contre les personnes, elles sont incriminées par l'art. 222-17 CP, qui aggrave la sanction si la menace est une menace de mort. Les articles R.631-1, R.634-1 et 322-12 CP incriminent les menaces simples de détruire, dégrader ou détériorer des biens. Si cette action avait pour conséquence de ne causer qu'un dommage léger, l'infraction est une contravention de la 1ère classe ; si le dommage devait être plus important, l'infraction est une contravention de la 4ème classe lorsque l'action ne ferait courir aucun danger pour les personnes et c'est un délit lorsque ce danger existerait.

Mais ces menaces constituent des infractions que si elles sont réitérées ou matérialisées " *par un écrit, une image ou tout autre objet* ". Or, peut-on affirmer qu'une menace proférée par Internet est matérialisée ? Se pose la question de savoir s'il faut pour cela que la menace soit imprimée, copiée sur une disquette ou s'il suffit qu'elle soit consultable sur le réseau. Nous pensons que cela suffit à matérialiser la menace, dès lors qu'elle n'a pas été supprimée par son auteur. C'est d'ailleurs la solution retenue par un Tribunal Correctionnel qui condamna à 2 mois d'emprisonnement avec sursis un propriétaire de pitbulls ayant adressé des menaces de mort à l'égard du député A. Santini sur le site web de ce dernier[63]. Il faudra alors veiller à identifier de façon certaine son auteur, car rien n'est plus facile que de se faire passer pour quelqu'un autre sur Internet.

Les menaces sous condition

---

[58] " A l'attaque des world companies " Le Monde Cahier Multimédia 1er-2 mars 1998
[59] Crim.12 oct. 1976 Bull. Crim. n°287
[60] Crim. 8 fév. 1994 Bull. Crim. n°58
[61] " Les délits boursiers sur l'Internet " Les Echos 18 déc. 1997
[62] " Internet au bord de la crise à cause d'un tueur virtuel " Marianne n°42 9-15 fév. 1998
[63] jugement du 28 avril 1998 – http://www.legalis.net – solutions identiques par des juridictions étrangères : condamnation d'un Danois à une amende de 2 000 couronnes pour avoir envoyé des menaces de mort à un journaliste via Internet (Le Monde 2 sept 1998) ;condamnation à un an d'emprisonnement d'un étudiant américain ayant menacé de mort d'autres étudiants (informations de mai 98 http://www.legalis.net)

Ces menaces, qui se distinguent également selon l'objet de l'infraction que l'auteur menace de réaliser, sont sanctionnées plus sévèrement que les précédentes car elles imposent à la victime l'obligation de remplir une condition.

Si la menace porte sur la commission d'un crime ou d'un délit contre les personnes, l'art. 222-18 CP prévoit une peine d'emprisonnement de 3 ans et une amende de 300 000 F. Cette peine est de 5 ans et 500 000 F lorsque la menace est une menace de mort.

Il existe deux infractions que l'on pourrait rapprocher de cette infraction, voire considérées comme des applications de la première dans certaines hypothèses : l'extorsion (art. 312-1 CP) et le chantage (art. 312-10 CP). En effet, l'extorsion est constituée par *une menace de violence* et le chantage la *une menace de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération.* Ces menaces sont formulées *sous condition pour la victime de faire bénéficier autrui d'une signature, un engagement ou une renonciation, de révéler un secret ou de remettre des fonds, des valeurs ou un bien.* Il est intéressant de noter que les sanctions sont alors beaucoup plus importantes (7 ans d'emprisonnement et 700 000 F d'amende pour l'extorsion et 5 ans d'emprisonnement et 500 000 F d'amende pour le chantage).

L'art. 322-13 CP réprime quant à lui la menace de commettre une infraction contre les biens citée plus haut sous condition. Le fait que cette infraction pourrait être dangereuse pour les personnes constitue une circonstance aggravante.

Les menaces peuvent enfin être rapprochées de la communication ou de la divulgation de fausses informations. Ces dernières sont incriminées lorsqu'elles font croire à la commission, passée ou à venir, d'une destruction, dégradation ou détérioration dangereuse pour les personnes, ou à la réalisation d'un sinistre (art. 322-14 CP). Est également incriminé le fait de compromettre la sécurité d'un aéronef en vol ou d'un navire par une telle information (art. 224-8 CP). Il faut noter que pour que ce dernier comportement constitue une infraction, il est nécessaire que l'auteur mette en jeu la sécurité de ces moyens de transport et qu'il en ait conscience. Une telle information, divulguée sur Internet, ne pourrait donc être pénalement réprimée que si l'auteur la communique directement, par courrier électronique ou sur leur serveur, à des personnes intéressées par la sécurité de l'aéronef ou du navire (autorité de police, compagnie aérienne..), ou éventuellement s'il la communique à un large public (en avertissant une agence de presse par e-mail, en laissant un message pirate sur un serveur très consulté comme un moteur de recherche..).

CHAP. II. L'INFORMATION, OBJET DE L'INFRACTION

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 (Sect°I.). Le droit pénal français peut répondre à cette nécessité (Sect°II.).

SECT°. I. -LA NECESSITE D'UN ARSENAL JURIDIQUE

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[1].

[1] " 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

Nous nous attacherons à la délinquance assistée par ordinateur. 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.

§1. LES ATTAQUANTS

Les attaques des "pirates" informatiques ne sont pas toujours menées, même si elles le sont souvent, dans un but financier (A.) mais toutes ces attaques ont une répercussion financière importante sur leurs victimes (B.).

A. LES MOTIVATIONS DES FRAUDEURS

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[2] poussa les criminologues à s'intéresser aux motivations des délinquants informatiques[3]. 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.

A la suite des "*phreakers* "[4] qui utilisaient le téléphone pour se connecter aux ordinateurs, sont apparus les "*hackers*" et les "*crackers*" qui eux agissent par le biais d'Internet. Dorénavant, 80 % des connexions pirates[5] utilisent ce support. Ces pirates, s'ils emploient les mêmes méthodes, ne poursuivent pas les mêmes buts.

I. LES " HACKERS "

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[6]. Ce sont des "entrepreneurs" selon la classification de Philippe Rosé[7], 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.

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[8]. 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[9]. On peut même accéder sur Internet à un musée des meilleurs piratages d'un groupe de "hackers"[10] sur lequel figure entre autre celui du site de la CIA, rebaptisée à l'occasion "Central Stupidity Agency" et où figurent insultes et liens hypertextes avec des sites pornographiques.

---

[2] 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.

[3] *La criminalité informatique* P. Rosé – éd. PUF 1988 – *La sécurité informatique* C. Jan & G. Sabatier – éd. Eyrolles 1989

[4] 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* ")

[5] selon un enquête du FBI – *Guerres dans le cyberspace* J. Guisnel – ed. La Découverte / Poche 1997

[6] 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

[7] *La criminalité informatique* P. Rosé – éd. PUF 1988

[8] " 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

[9] " 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 juill 1998

[10] http://www.dis.org

II. 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* "[11].
Ils sont d'autant plus dangereux qu'ils s'échangent leurs techniques au sein de newsgroups spécialisés ou par l'intermédiaire de revues[12] distribuées par mailing lists. Ils vont même jusqu'à former des clubs tel le Chaos Computer Club de Hambourg[13] ou le CLODO en France (Comité Liquidant Ou Détournant les Ordinateurs). Désormais, ils représentent 90% des attaquants.

Les "agressifs"[14] 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 paragouvernementaux recherchent à obtenir divers renseignements (du secret-Défense aux renseignements industriels, diplomatique..) relatifs à certains Etats, ou ils peuvent attenter au 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[15].
Des entreprises agiront de même à l'égard de leurs concurrents. Ainsi, on peut citer l'exemple[16] 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. 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* "[17]. Fin 1997, on a craint une telle attaque[18] : 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 le *New York Times* un jour de consultation importante[19]. C'est également pour des raisons idéologiques que certains Espagnols saturent les sites Internet de l'organisation séparatiste basque ETA[20].
L'attaque terroriste : Leurs auteurs tentent de déstabiliser l'ordre établi par des attaques spectaculaires[21].
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.

---

[11] *La bible Internet* Ed. Krol (traduction P. Cubaud & J. Guidon) coll. Guide & Ressources éd. O'Reilly international Thomson 1995
[12] " Phreack ", " 2600 ", " Computer Underground Digest " …
[13] qui, en 1986, pénétra dans plus de 135 réseaux dans 9 pays industrialisés.
[14]. *La criminalité informatique* P. Rosé – éd. PUF 1988
[15] P. Rosé " Délinquance informatique, inforoutes et nouvelle guerre de l'information " - Cahiers de la Sécurité Intérieure n°24
[16] " Cyberwars : la montée du crime informatique " Les Echos 10 fev 1998
[17] " 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
[18] " Pants/Hagis, le pirate de Noël menace Internet d'une bombe à retardement " Le Monde 12 déc 1997
[19] " Les pirates du cyberespace s'emparent du New York Times " Le Monde 16 sept 1998
[20] Le Monde 26 nov. 1997
[21] 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)

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*)[22]. 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.

B. LE COUT DE LA FRAUDE

Pour l'instant, aucune étude spécifique au coût des attaques via Internet n'a eu lieu. On peut cependant s'inspirer des coûts de la délinquance informatique en général pour envisager l'importance qu'elles pourront revêtir. Selon les chiffres du CLUSIF (Club de la Sécurité informatique français) de 1996[23], les actes de malveillance non matérielle en matière informatique représentent 7,6 milliards de francs, soit 60 % des pertes informatiques. Certains exemples des sommes qui peuvent être détournées par l'utilisation d'un ordinateur, et notamment par Internet sont impressionnants. D'ailleurs, 19 % des fraudes informatiques (en France) entraînent un préjudice de plus d'un million de francs[24]. Ainsi, des pirates russes ont passé un ordre de virement truqué de 80 millions de francs auprès d'une banque de Zurich et simultanément un ordre d'achat de diamants à Moscou pour la même somme. Le record est pour l'instant celui d'un sabotage du système informatique d'une mutuelle : la destruction des fichiers, programmes et sauvegardes a coûté 250 millions de francs[25].
Il ne faut pas négliger les conséquences non monétaires : si l'on parvient à s'infiltrer dans le système interne d'une entreprise, dans un système domotique ou autre, les répercussions peuvent être non seulement financières, mais aussi humaines. Par exemple, en octobre 1992, une panne générale de 36 heures de la centrale d'intervention, commandée par un ordinateur, du service d'ambulance de Londres entraîna le décès de 20 patients[26]

Mais on peut penser que ces chiffres ne révèlent pas l'exacte étendue de cette fraude. Le commissaire Padoin qui dirige le SEFTI[27] parle d'un chiffre noir de 90 %.
Effectivement, les victimes des fraudes sont souvent de grandes entreprises, des banques ou même des services étatiques. Elles préfèrent donc ne pas entacher leur image en révélant une perte importante ou ne serait ce que l'intrusion dans leur système : certaines font de l'inviolabilité de leur système un atout commercial. Parfois, elle préféreront se taire plutôt que de voir un policier intervenir et éventuellement découvrir des pratiques d'entreprise contestables. Il se peut de plus que les responsables de ces entreprises ou organismes n'aient pas connaissance de la fraude pour la simple raison que le directeur informatique ait préféré de leur cacher l'intrusion de peur de perdre son emploi. Parfois, c'est ce dernier qui ignore le piratage.

Selon le commissaire Marcel Vigouroux, qui est à la tête de la Brigade de Recherche et de Répression de la Criminalité Informatique, il faudrait s'inspirer de la solution adoptée en matière automobile pour avoir à la fois une meilleure connaissance du phénomène et voir baisser le nombre des infractions : Il s'agirait de subordonner le versement de l'indemnité par l'assurance au dépôt d'une plainte aux autorités de police[28].

§2. LES TECHNIQUES D'ATTAQUE

[22] 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
[23] Confidentiel et Sécurité n°33 avril 1997
[24] " Aspects de la criminalité et de la délinquance constatées en France en 1995 " Ministère de l'Intérieur Documentation Française
[25] " Cyberwars : la montée du crime informatique " Les Echos 10 fev 1998
[26] " Le nouvel article du code pénal suisse sur les virus informatiques " C.G. Frigerio – Rev. Int. de police Criminelle n°464 1997 p.19
[27] Service d'enquêtes sur les Fraudes aux Technologies de l'Information
[28] " Sur le front de la nouvelle criminalité " - interview du Commissaire Vigouroux – Expertises n° 183 – c'est d'ailleurs l'avis avancé dans le Rapport du Ministère de l'intérieur de 1995 sur les Aspects de la criminalité et de la délinquance constatée en France.

Ces pirates se fondent sur deux "postulats de la délinquance informatique "[29] 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[30] : 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[31] :

♦ **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

♦ **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 -** Il existe près de 12 000 virus dans le monde PC, 6 nouveaux étant créés par jour[32].

On distingue les virus selon leurs effets[33] :

- 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[34])
- 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

♦ **Le ver -** C'est un programme qui se déplace à travers le réseau et qui cherche à le perturber en le rendant indisponible (Internet a connu un ver en 1988).

♦ **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.

---

[29] P. Rosé " Délinquance informatique, inforoutes et nouvelle guerre de l'information " - Cahiers de la Sécurité Intérieure n°24

[30] " Attaques par les données " I. Vassileff http://www.grolier.fr/cyberlexnet – " La menace et les attaques informatiques " note du 28 mars 1994 du SCSSI

[31] 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

[32] " 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

[33] *Internet pour les juristes* N. Tortello & P. Lointier éd. Dalloz

[34] Le Monde 23 janv 1998

♦ **Le *cookie*[35] -** Lorsque l'on se connecte à un serveur, celui-ci peut fixer sur le disque dur de l'ordinateur connecté un fichier qui retracera le parcours de l'utilisateur sur le site. A la prochaine connexion, ce fichier s'active et transmet au serveur les informations enregistrées.

SECT°. II. LE CONTENU DE L'ARSENAL JURIDIQUE

[35] *Le projet Intranet* F. Alin, D. Lafont & J.F. Macary éd. Eyrolles 1997

Le projet du Nouveau Code Pénal[1] prévoyait d'incriminer de façon distincte chacune de ces attaques. Le projet présentait en effet quatre "formes d'atteintes graves à des systèmes informatiques " et à chacune d'entre elles un article étant associé.

- **l'accès frauduleux à un programme :** le projet comble à cet égard un vide juridique en incriminant le fait de capter frauduleusement un programme, une donnée ou tout autre élément d'un système de traitement automatique d'information
→ *"le fait de capter frauduleusement un programme, une donnée ou tout autre élément de traitement automatique d'informations est puni de trois ans d'emprisonnement et de 1 000 000 F d'amende"*
- **l'espionnage informatique** peut se concrétiser de manière encore plus nette par l'utilisation, la communication ou la reproduction d'un programme, d'une donnée ou de tout autre élément d'un système de traitement informatique
→ *"le fait, au mépris des droits d'autrui, d'utiliser, de communiquer ou de reproduire un programme, une donnée ou tout autre élément d'un système de traitement automatique d'informations est puni de trois ans d'emprisonnement et de 1 000 000 F d'amende"*
- **le sabotage informatique** peut causer un préjudice inestimable à l'utilisateur. Ce risque apparaît d'autant plus grave que tout informaticien est en mesure, au moyen d'une " bombe logique ", de détruire totalement ou de rendre inutilisable la mémoire d'un ordinateur, ou peut fausser le traitement en altérant une donnée ou un élément de programme
→ *"le fait, intentionnellement et au mépris des droits d'autrui, de détruire ou d'altérer tout ou partie d'un système de traitement automatique d'informations, ou d'en entraver ou fausser le fonctionnement, est puni de cinq ans d'emprisonnement et de 2 500 000 F d'amende"*
- **les malversations :**un système de traitement informatique peut être utilisé dans la perspective de commettre des malversations.
→ *"le fait, en utilisant frauduleusement un système de traitement automatique d'informations, d'obtenir ou de faire obtenir à autrui un profit illicite est puni de cinq ans d'emprisonnement et de 2 500 000 F d'amende"*

Mais les parlementaires préférèrent conserver les incriminations de la loi Godfrain du 5 janvier 1988.

Il faut de plus indiquer qu'un débat eu lieu sur le point de savoir dans quelle partie du Nouveau Code Pénal devaient être situées les infractions en matière informatiques.
Initialement placées dans le Livre III relatif aux crimes et délits contre les biens, les art. 323-1 & s. y demeurèrent malgré la demande de la Commisssion des Lois sénatoriale[2] de les placer, ainsi que les règles relatives à la protection des informations nominatives, dans un livre V. Ce dernier aurait été un livre "relatif au droit pénal spécial". Comme l'a dit M. Thyraud[3] "*autant dire que ne pas faire entrer la fraude informatique dans la discussion du livre III reviendrait en reporter la discussion à une échéance d'une dizaine d'années, car les livres du droit pénal spécial ne seront pas promulgués au fur et à mesure de leur adoption../..Il y eut une époque où l'informatique était, je le reconnais, un monde à part. On aurait pu alors lui réserver un sort particulier en tant que technologie autonome. Elle aurait pu figurer sans inconvénient dans le droit pénal spécial avec l'urbanisme, la santé, l'environnement ou le droit bancaire../.. cette époque est révolue. L'informatique participe à la complexité de la vie moderne pour en réguler les effets. Elle est si intégrée aux activités de notre société qu'elle se confond avec elle.*".

Ainsi, grâce à la prise de conscience du législateur de la place prépondérante de l'informatique, nous avons un arsenal juridique complet qui permet d'assurer le respect de la confidentialité (§1) et de l'intégrité (§2) de l'information. Il est important de préciser avant d'étudier cet arsenal que la plupart des incriminations présentées peuvent donner lieu à des poursuites pour tentative, ainsi qu'à l'égard des personnes morales. De plus, la sanction de la confiscation de l'objet ayant servi à l'infraction est prévue dans la plupart des cas.

§1. LE RESPECT DE LA CONFIDENTIALITE DE L'INFORMATION

Afin de sanctionner l'atteinte à la confidentialité de l'information qui circule sur Internet ou que l'on dérobe dans un ordinateur en passant par Internet, le juge peut condamner pour avoir appréhendé l'information (A.) ou pour avoir utilisé l'information, ce qui implique l'appréhension préalable (B.).

[1] projet de nouveau de code pénal n°215 J.O. du Sénat 15 fév 1989
[2] Rapport de la Commission des lois devant le Sénat n°54 J.O. du Sénat 23 oct. 1991
[3] débats parlementaires devant le Sénat J.O. du Sénat 29 oct 1991 p.3351

A. LA CONNAISSANCE DE L'INFORMATION

Si le vol d'information a été rejeté de façon claire (I.), d'autres incriminations permettent de poursuivre la prise de connaissance illégitime de l'information (II.).

I. L'EXCLUSION DU VOL D'INFORMATION

Selon la conception traditionnelle du vol, l'information ne pouvait être concernée par cette infraction. A partir des années 80 la question redevint d'actualité évidemment en raison de l'émergence de l'information dans notre société mais surtout de la poursuite de mouvement d'extension du domaine du vol et d'une jurisprudence touchant particulièrement à ce type de biens, jurisprudence dont certains ont dit qu'elle consacrait le vol d'information. L'arrêt Logabax du 8 janvier 1979[4] ainsi que surtout les arrêts Bourquin du 12 janvier 1989[5] et Antoniolli du 1er mars 1989[6] sont à l'origine de cette position soutenue par M. Catala[7] et Mme Lucas de Leyssac[8]. La Chambre Criminelle de la Cour de Cassation avait en effet refuser de casser les arrêts de condamnation pour vol rendus par des Cours d'Appel à l'encontre d'employés ayant " emprunté " des disquettes à leur employeur pour en copier le contenu (la liste des clients) ou utilisé des documents de leur employeur pour établir des fiches de renseignements au profit d'un concurrent.

Il est sans doute exact que la Chambre Criminelle s'est servie du prétexte du vol momentané du support de l'information pour sanctionner en pratique "le vol d'information ". Mais cela ne veut pas dire pour autant qu'elle soit favorable à la théorie du vol d'information.

Certes, les arrêts Bourquin et Antoniolli pouvaient être interprétés en faveur du vol d'information. Mais l'ambiguïté des termes employés pouvait également être utilisée en faveur de la thèse contraire : l'on trouve des expressions telles que "*Antoniolli a usurpé la possession de ces documents* "[9] ou des exposés de motifs indiquant que les prévenus n'ont fait "*d'une part qu'appréhender l'original ou la première copie de sauvegarde pour en faire une reproduction./. et d'autre part, sorti de l'entreprise les disquettes* "[10], expressions qui pourraient être comprises comme excluant toute appropriation d'informations. Ces deux arrêts condamneraient donc plutôt au vol du support de l'information, vol momentané, le temps de la reproduction selon la jurisprudence Logabax.

De plus, ces deux arrêts sont des arrêts de rejet par lesquels la Cour de Cassation ne fait que reprendre l'exposé des motifs des Cours d'Appel. Elle rejette dans l'affaire Bourquin des pourvois invoquant des arguments de procédure et dans l'affaire Antoniolli un pourvoi qui tendait à contester une appréciation souveraine des juges du fond (il est vrai que la Cour de Cassation aurait pu éviter cette controverse en opérant une substitution de motifs).

De plus, de l'avis de tous, la Chambre Criminelle vient d'exclure toute possibilité d'incriminer le vol d'information dans son arrêt du 3 avril 1995[11]. Le " Canard Enchaîné " ayant publié la reproduction partielle, en fac similé, de trois avis d'imposition de J.Calvet, sur laquelle figurait le montant déclaré de ses revenus, des membres du journal furent poursuivis pour recel d'information. La Cour d'Appel avait exclu cette prévention, lui préférant celle de recel de photocopies provenant de la violation du secret fiscal pour laquelle elle condamna les prévenus. La Chambre Criminelle prit le soin de confirmer cette exclusion, ce qui montre sa volonté de rejeter tout recel et donc vol d'information : " *Une information, quelle qu'en soit sa nature ou l'origine, échappe aux prévisions tant de cet art. 460 que de l'art. 321-1 du Code Pénal entré en vigueur le 1er mars 1994* ". Notons qu'il reste à voir si ce rejet du recel d'information est fondé.

La rédaction du Code Pénal entré en vigueur en 1994 fut également l'occasion pour le législateur d'écarter toute possibilité de vol d'information.

La version originale du projet de nouveau code pénal[12] prévoyait un article 307-1 qui incriminait " *le fait de capter frauduleusement un programme, une donnée ou tout autre élément d'un système de traitement automatique d'informations* ", comportement puni de trois ans d'emprisonnement et de 1 000 000 francs

[4] D. 1979 p.509
[5] Bull. Crim. 1989 n°14 – Expertises n°119 p.269
[6] Bull. Crim. 1989 n°100
[7] Catala - " Ebauche d'une théorie juridique de l'information " - D.1984 chron. p.97
[8] M.P. Lucas de Leyssac - " L'arrêt Bourquin,une double révolution : un vol d'information seule,une soustraction permettant d'appréhender des reproductions qui ne constitueraient pas des contrefaçons " - RSC juill-sept 1990
[9] arrêt Antoniolli
[10] arrêt Bourquin
[11] Bull. Crim. 1995 n°142 - D.1995 somm.320 - Rev.Sc.Crim. 1996.645 - JCP 1995.II.22429
[12] projet de loi n°215 J.O. du Sénat 15 fév 1989

d'amende. Mais cette incrimination fut écartée dès la première lecture du projet par le Sénat[13]. La Commission des lois devant l'Assemblée Nationale[14] résume la raison de ce rejet à des difficultés juridiques et une inutilité de l'incrimination. En ce qui concerne les difficultés juridiques, elle indique que " *la notion de soustraction ne peut s'appliquer à la copie d'une donnée informatique – l'information volée restant entre les mains de son détenteur original* " et de plus, " *le vol implique une atteinte à la propriété alors que l'information, n'appartient pas à son détenteur et n'est pas un bien susceptible d'appropriation* ". Quant à l'inutilité de l'incrimination, la Commission souligne que "*la notion de vol ne paraît pas indispensable pour assurer une protection de l'investissement des producteurs d'information* " car il existe d'autres dispositions.

II. LES SOLUTIONS

1. Un texte particulier

L'art. 226-15 CP qui sanctionne d'un an d'emprisonnement et de 300 000 F d'amende " *le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications* " apparaît a priori comme applicable à certains services d'Internet comme le courrier électronique.
De ce fait, d'autres services sont exclus de la protection de cet article offert aux correspondances.
Mais le courrier électronique est-il lui-même vraiment une correspondance émise par voie de télécommunications ? Nous verrons ultérieurement que si la réponse logique à cette question est positive, cela entraîne bon nombre de difficultés juridiques, notamment en matière de responsabilité des acteurs du réseau.

D'où la nécessité de recourir dans toutes les hypothèses aux dispositions relatives aux atteintes aux systèmes de traitement automatisé de données.

2. Un texte général

Les dispositions de l'art. 323-1 CP furent créées par la loi Godfrain du 5 janvier 1988. Ce texte avait pour but de prendre en compte l'émergence de l'informatique et les dangers qu'elle peut représenter.
L'une de ces dispositions sanctionne la prise de connaissance illégitime de l'information, mais de façon détournée. En effet, l'art. 323-1 énonce que " *le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende* ". Ce n'est pas la prise de connaissance que ce texte réprime, mais l'accès ou le maintien frauduleux dans le système, qui impliquent l'un comme l'autre la prise de connaissance de l'information. Nous avons déjà vu que les parlementaires avaient refusé d'incriminer " *le fait de capter frauduleusement un programme, une donnée ou tout autre élément d'un système* ", de peur de sanctionner par trop directement " le vol d'information ". Notons que le changement d'incrimination lors des débats a entraîné un changement de sanctions : nous sommes passé d'une peine d'emprisonnement de 3 ans et surtout d'une amende de 1 000 000 F à une peine d'un an d'emprisonnement et de 100 000 F d'amende.

Deux éléments matériels doivent être réunis pour constituer l'infraction. il s'agit d'un accès ou d'un maintien, dans un système de traitement automatisé de données.

Le ***système de traitement automatisé de données*** est l'objet de l'accès ou du maintien. Pour certains auteurs comme le professeur Gassin, il constitue une condition préalable.

La proposition de loi de M. Godfrain visait initialement un " système de traitement de l'information " mais la Commission sénatoriale lui préféra l'expression que nous connaissons car elle permettait une interprétation plus large. Cette commission en donna également une définition : " *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* ", mais cette définition ne fut formulée dans le texte d'incrimination ni en 1988, ni lors de la rédaction du Code Pénal de 1994. L'objectif du législateur a toujours été, face à une expression empruntant à la technologie de l'envisager dans un sens très large. Le sénateur Thyraud[15] disait lui-même que cette définition était destinée à couvrir " *la situation la plus simple, l'ordinateur isolé, et la plus complexe, le réseau aux multiples ramifications qui fait le*

[13] Débats parlementaires devant le Sénat J. O. du Sénat 30 oct. 1991 p. 3422
[14] Rapport de la Commission des lois devant l'AN n° 2468 J. O. de l'AN 12 déc. 1991 p.118
[15] Rapport de la Commission des lois devant le Sénat n°214 J.O. du Sénat 1987-1988

tour de la terre ". Certains auteurs[16] considéraient que les réseaux ne pouvaient pas être compris dans ce vocable de " système ", constituant eux-mêmes des systèmes de systèmes. Ce à quoi la majeure partie de la doctrine et les parlementaires ont répondu qu'un système de systèmes constitue bien un système et qu'exclure les réseaux de l'incrimination reviendrait à " *rogner les ailes et ôter toute portée véritable* "[17] aux dispositions de la loi Godfrain.

Le texte vise deux types de comportements, qu'un auteur[18] distingue comme l'accès dans l'espace et l'accès dans le temps. Il s'agit de ***l'accès et du maintien***.

A l'instar de l'incrimination d'intrusion frauduleuse sur un terrain, un engin ou un appareil militaire (art. 413-5 CP), cette infraction est une infraction-obstacle, qui incrimine un comportement sans suite dommageable directe mais pour prévenir la commission d'une autre infraction.

Quant à **l'élément moral**, c'est non seulement la volonté de violer la loi pénale comme pour tout délit, mais aussi d'agir frauduleusement. Cette exigence est confirmée par la définition officieuse du " système.. " : nous avons vu que la Commission du Sénat avait retenu une définition exigeant du système qu'il soit " *protégé par des dispositifs de sécurité* ", condition qui fut exclue. De ce fait, " *l'absence de protection sérieuse du système, la négligence des gestionnaires ou des utilisateurs ../..ne saurait constituer une excuse pour les ''hackers''* "[19].

B. L'UTILISATION DE L'INFORMATION

Incriminer la connaissance de l'information et rapporter la preuve de celle-ci est relativement difficile comme nous l'avons vu. Dès lors que le délinquant utilise l'information, il n'y a plus de doute en ce qui concerne l'appréhension de l'information. C'est pourquoi il est plus facile de poursuivre ce comportement dans ce contexte.

Nous étudierons plus précisément la constitution de fichiers et de traitements informatiques (I.) et le recel d'information (II.).

Auparavant, il faut rappeler que des poursuites sur le fondement de la contrefaçon sont également envisageables. Celles-ci se justifient dans la mesure où l'utilisation de l'information, qui doit pour bénéficier de cette protection répondre à l'exigence d'originalité, porte atteinte à la rémunération de son auteur. Nous ne reviendrons pas sur cette infraction qui a déjà fait l'objet de développements[20].

I. LES FICHIERS ET TRAITEMENTS INFORMATIQUES

Cette protection ne peut porter que sur les données nominatives.

Nous avons déjà vu qu'Internet peut être utilisé pour divulguer des informations nominatives. Il peut aussi être utilisé pour constituer les fichiers de ces données.

On pense notamment aux informations qui peuvent être communiquées grâce à l'utilisation de *cookies*[21]. En principe, les *cookies* activent le fichier contenant les informations relatives aux connexions de l'utilisateur au serveur l'ayant introduit lorsque l'utilisateur se reconnecte au dit serveur. Cela permet au serveur de personnaliser l'échange avec l'utilisateur en devançant ses attentes. Mais le danger est que ces informations, transmises par l'ordinateur de l'utilisateur le temps de la connexion, soient conservées par le destinataire. Pire, que ce dernier vendent ces fichiers ou permettent à d'autres serveurs d'accéder aux informations enregistrées grâce aux *cookies*. Dès lors, les gouvernements, les employeurs, les commerçants pourraient établir des bases de données sur un citoyen, un employé, un consommateur, soit pour mieux le surveiller, soit pour mieux cerner sa cible. En effet, les employeurs peuvent ainsi vérifier que leurs employés n'utilisent pas l'ordinateur pour aller sur

[16] R. Gassin " La protection pénale d'une nouvelle " universalité de fait " en droit français : les sytèmes de traitement automatisé de données " Actualité législative Dalloz 1989 P. 5 à 65

[17] *La fraude informatique* G. Champy éd. Presses Universitaires d'Aix-Marseille 1992 p. 144

[18] *La fraude informatique* G. Champy éd. Presses Universitaires d'Aix-Marseille 1992 p. 160 & s.

[19] Rapport de la Commission des Lois devant l'Assemblée Nationale n°2468 J.O. de l'AN 12 déc 1991

[20] voir " la contrefaçon " p.29

[21] pour voir un exemple d'application : http://www.cnil.fr. – " De la protection de la vie privée : des cookies indigestes " G. Betoun http://www.grolier.fr/cyberlexnet – " Les cookies : big browser is watching you " I. Vassileff http://www.grolier.fr/cyberlexnet

des sites " de charme " ou des casinos virtuels au lieu de travailler. Les commerçants qui proposent leurs marchandises sur le réseau peuvent connaître de cette manière les goûts de leurs acheteurs et ainsi adapter leurs offres à sa personnalité.

Nous avons déjà étudié les dispositions générales relatives au traitement informatisé des informations nominatives. Les incriminations citées trouveront à s'appliquer car généralement, ces bases de données ne sont pas constituées, ni divulguées selon les exigences de la loi du 6 janvier 1978.

De plus, l'art. 226-18 CP est selon nous destiné à s'appliquer à l'utilisation de *cookies* pour établir ces fichiers. Il énonce que " *le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes est puni de 5 ans d'emprisonnement et de 2 000 000 F d'amende.* ". La question se pose également de savoir si le fait d'afficher sur l'écran, au moment de la connexion, un message prévenant l'internaute que le serveur installe des *cookies* et lui permettant d'en refuser l'installation, suffit à rendre cette méthode de collecte d'information licite.

Un avocat, Maître Betoun[22], estime de plus que l'art. 323-1 CP que nous avons déjà étudié est susceptible de s'appliquer.

II. LE RECEL D'INFORMATION

1. La tentative d'incrimination du recel de données informatiques

Le projet de Nouveau Code Pénal[23] définissait dans un art. 305-1 le recel comme "*le fait, pour une personne, au préjudice des droits d'autrui, de détenir, d'utiliser, ou de transmettre une chose en sachant que celle-ci provient d'une infraction. Constitue également un recel le fait pour une personne, dans les mêmes conditions, de faire office d'intermédiaire afin de transmettre la chose* ".

Le Sénat modifia cette définition. M. Thyraud considéra dès lors que des données ne pouvaient plus faire l'objet d'un recel puisque "*la donnée n'est pas un bien* ". Il fallait alors prévoir un texte particulier pour incriminer le recel de données. Ce fut l'art. 307-4-2[24] qui punissait le "*recel de données obtenues en violation* " des atteintes aux systèmes de traitements automatisés de données de 5 ans d'emprisonnement et de 2,5 millions de francs d'amende.

L'Assemblée Nationale modifia par la suite la définition du recel[25], qui devint : "*le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel, le fait, en connaissance de cause, de bénéficier par tout moyen, du produit d'un crime ou d'un délit* ". L'Assemblée remplaçait ainsi le notion sénatoriale d' "utilisation" par cette de " bénéfice du produit d'un crime ou d'un délit". Elle considéra dès lors, que l'incrimination de recel de données informatiques était superflue car susceptible d'être couverte par ce texte général, grâce à cette notion.

Dans un premier temps, la Commission du Sénat voulut lorsqu'elle rendit son rapport, réintroduire le recel de données en considérant que cette incrimination pouvait se révéler utile[26]. Puis durant les débats[27], la Commission se rallia à la définition générale du recel de l'Assemblée, et retira son amendement destiné à rétablir le recel de données informatiques.

2. L'application du recel ?

Les données informatiques sont le support d'informations. Or, le recel d'information est impossible selon la Chambre criminelle de la Cour de Cassation.

a) Le rejet jurisprudentiel du recel d'information

[22] G. Bitoun " De la protection de la vie privée : des cookies indigestes " http://www.grolier.fr/cyberlexnet
[23] Projet de loi n° 215 J.O. du Sénat 15 fevr 1989
[24] amendement n° 142 – débats parlementaires devant le Sénat 30 oct 1991
[25] Projet de loi n° 212 J.O. de l'AN 18 déc 1991
[26] Rapport de la Commission des Lois devant le Sénat n° 261 J.O. 26 fev 1992
[27] débats parlementaires devant le Sénat 22 avril 1992 – p. 756 & 765

Dans son arrêt du 3 avril 1995[28], la Chambre Criminelle a rejeté toute hypothèse de recel d'information. Deux journalistes étaient poursuivis pour avoir publié la reproduction partielle, en fac-similé, de trois avis d'imposition d'un chef d'entreprise, sur laquelle figurait le montant de ses revenus. Les poursuites avaient été ouvertes du chef de recel d'informations. Mais la Cour d'Appel les avaient condamnés sur le fondement, non de recel de vol ou de recel d'informations, mais de recel de photocopies provenant d'une violation du secret fiscal. La Chambre Criminelle confirma cet arrêt et pris le soin de souligner qu' " *une information, quelle qu'en soit la nature ou l'origine, échappe aux prévisions tant de cet art. 460 que de l'art. 321-1 du Code Pénal entré en vigueur le 1er mars 1994* ".

La volonté de la Cour de faire de cet arrêt un arrêt de principe est fortement marquée. A priori, la Cour semble dégager un principe pour l'avenir puisque, les poursuites ayant été engagées sur le fondement d'incriminations du Code Pénal de 1810, elle souligne que la solution demeurera après l'entrée en vigueur du Code Pénal de 1994. Mais cela n'interdit pas un revirement de jurisprudence par la Chambre Criminelle.

Mais la Cour de Cassation a-t-elle vraiment l'intention d'écarter le recel de toute information ? Malgré la formulation employée pour énoncer le principe rappelé, ne va-t-elle pas réserver un sort particulier aux informations à caractère secrètes ?

Effectivement, la jurisprudence considérait auparavant que le secret pouvait être recelé. Ainsi, peut être recelé un secret de fabrique[29], un secret de l'instruction ou de l'enquête[30]. L'arrêt du 3 avril 1995 semble considérer que désormais, même les informations secrètes en elles-mêmes ne pourront pas faire l'objet de recel. Pour toutes les informations, on devra distinguer deux hypothèses[31] : soit on produit un document – ou la photocopie d'un document - qui aura été obtenu de façon illicite et l'on est susceptible d'être poursuivi pour recel, soit on produit l'information, sans avoir recours au document qui la contient – ni à une copie- et l'on échappe à l'infraction.

Mais est-il vraiment impossible de concevoir le recel d'information ?

b) *Une conception du recel d'information*

Nous avons vu que les parlementaires étaient favorables au recel de données informatiques, les sénateurs voulant une incrimination spécifique et les députés modifiant le texte général sur le recel pour permettre cette incrimination.

Cette volonté du législateur s'exprime par la formulation de l'art. 321-1 CP qui permet tout à fait de viser une information. En effet, la nouvelle rédaction a consacré la jurisprudence qui avait fait évolué le recel de "recel - détention " en " recel - profit "[32]. C'est d'ailleurs ce qu'avait souligné le député M. Hyest, rapporteur de la Commission des Lois devant l'Assemblée Nationale : " *Cet amendement consacre la jurisprudence de la Cour de Cassation, qui incrimine le fait de bénéficier par tous moyens du produit d'un crime ou d'un délit, et qui a ainsi condamné la personne qui, en connaissance de cause, prend place dans une voiture volée* "[33]. L'avantage de cette conception du recel et de la formulation de ce second alinéa est qu'ils permettent de pallier au fait que " *la référence à l'utilisation de la chose* " du premier alinéa " *ne recouvre pas toutes les situations dans lesquelles il est tiré profit d'un tel produit* ".

Une information peut-elle donc être l'objet du recel visé par l'al. 2 de l'art. 321-1 qui énonce que "*Constitue également un recel, le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit*" [34]? La difficulté de cette question se situe au niveau des éléments matériels de l'incrimination.

" bénéficier, par tout moyen "

Ce bénéfice ne signifie pas forcément une augmentation du patrimoine. Le cas échéant, détenir une information peut enrichir le patrimoine, mais cela peut permettre également de voir diminuer le patrimoine d'un concurrent ou de lui porter atteinte. Le receleur en tirera tout de même un profit, quelque soit sa forme, ce qu'autorise l'expression "*par tout moyen*".

De plus, selon la jurisprudence dégagée avant l'entrée en vigueur du Code Pénal de 1994, le recel ne nécessite pas de détenir matériellement ce produit. C'est ainsi qu'est coupable de recel celui qui

[28] Crim. 3 avril 1995 – Bull. Crim. N° 142 – JCP 1996 éd. G. I. 3909 chron. M. Véron n°5 – D. 1995, somm. p.320 note M.Pradel – Expertises n°183 p. 189 & 196 note A. Weber
[29] Crim. 7 nov 1974 – Bull. Crim. N°323
[30] Crim. 13 mai 1991 – Bull. Crim. N°200 – D. 1993 somm.17 – Rev. Sc. Crim. 1992, 312
[31] *Droit Pénal Spécial* M. Véron coll. U éd. Masson 1996
[32] Crim. 9 juill. 1970 Bull. Crim. 236
[33] Débats parlementaires devant l'Assemblée Nationale J.O. de l'AN 17 déc. 1991 p.8072
[34] *La fraude informatique* G. Champy éd. Presses universitaires d'Aix-Marseille 1992 tome II p. 778

bénéficie du règlement de ses propres créanciers, effectué directement par l'auteur de l'infraction d'origine d'où proviennent les fonds[35].

" du produit "

Le choix du terme "produit" et non de "chose" est délibéré, nous l'avons vu. Il s'agissait de pallier au domaine restrictif du premier alinéa déterminé par le terme "chose" qui exclut élément incorporel.

Notons que l'on peut se demander si le terme de "chose" est d'ailleurs approprié[36]. Certes, l'objet du vol ne peut être qu'une chose, mais le recel est une infraction autonome depuis la loi du 22 mai 1915. Depuis cette date, le recel peut être la conséquence de tout autre infraction comme l'indique l'incrimination qui vise les choses qui proviennent "*d'un crime ou d'un délit*" sans distinction. Il en est ainsi par exemple de l'escroquerie[37], ou d'un abus de confiance[38]. Or ces infractions peuvent avoir pour objet non seulement une chose mais également des fonds, des valeurs ou un bien quelconque, un service, le consentement à un acte opérant obligation ou décharge (pour ne prendre que l'exemple de l'escroquerie). Comme l'écrit Mme Rassat, " *Ce mot est imparfait car il évoque un objet corporel alors que le recel, parce qu'il concerne tous les biens de provenance délictueuse a toujours pu s'appliquer à un bien incorporel du moment que celui-ci pouvait entrer dans le cadre de l'infraction d'origine* ".

En ce qui concerne le produit, il peut être de toute nature puisque la loi n'ayant pas distingué, il n'y a pas à distinguer. De plus, le terme de "produit" indique que l'objet du recel n'est pas forcément le même objet que celui de l'infraction originelle. Ainsi, on peut non seulement profiter de l'argent subrogé à l'objet de l'infraction initiale, mais aussi d'une place de passager dans une voiture volée[39], du train de vie de son conjoint résultant d'un détournement[40], de l'augmentation de la valeur des actions d'une société dont on est actionnaire si celle-ci bénéficie d'un accroissement de l'actif du fait d'un abus de bien[41]. En matière d'atteinte aux systèmes de traitement automatisé des données, l'infraction qui serait la plus souvent susceptible d'être accompagnée d'un recel est celle qui est prévue par l'art. 323-1 : " *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ". Cette incrimination décrit le comportement de celui qui s'immisce dans un système, généralement pour prendre connaissance de données confidentielles. Ces informations pourraient faire l'objet de recel. Or, l'objet de l'infraction d'accès ou de maintien frauduleux est, non pas l'information, mais le système de traitement. Malgré cela, il pourra y avoir recel.

" d'un crime ou d'un délit "

L'infraction originelle peut être toute infraction, à l'exclusion d'une contravention. Or les infractions d'atteinte aux systèmes de traitement automatisé des données sont des délits. Le produit de ces infractions peut donc faire l'objet d'un recel.

Notons que si l'on reconnaissait ce type de recel, l'auteur de l'accès ou du maintien frauduleux ne pourrait pas être poursuivi comme receleur, selon la jurisprudence qui considère que l'infraction originelle et le recel sont exclusives l'une de l'autre[42]. Cependant, si une telle solution se justifie en matière de vol ou d'escroquerie, car l'auteur de ses infractions a l'intention de profiter de l'objet de son acte, ce qui ferait double emploi avec le recel, on peut douter de l'application à l'accès ou au maintien frauduleux de ce raisonnement. En effet, cet article, même s'il permet de poursuivre celui qui prend connaissance de données confidentielles, n'a pas que ce but : il permet de poursuivre plus simplement celui qui s'introduit dans un système, ne serait-ce que pour s'y introduire (même si nous pouvons nous douter que le Parquet ne l'utilisera que dans la première hypothèse, faute de gravité et de temps pour traiter la seconde). Les parlementaires ont d'ailleurs écarté du projet de loi une incrimination permettant de sanctionner exclusivement le "vol" de données[43]. Aucune volonté de profiter des données n'étant requise par l'art. 323-1, on peut penser que des poursuites pour recel ne seraient pas incompatibles.

§2. LE RESPECT DE L'INTEGRITE DE L'INFORMATION

Le respect de l'intégrité de l'information est protégé par l'incrimination de l'atteinte à l'intégrité des données informatiques (A.) et du faux (B.).

---

[35] Crim. 19 avril 1996 – Bull. Crim. n° 174
[36] *Les infractions contre les biens et les personnes dans le Nouveau Code Pénal* M.L.Rassat coll. Services Dalloz n° 130
[37] Crim. 18 janv 1988 – Bull. Crim n°22
[38] Crim. 16 juill 1964 – Bull. Crim n°241
[39] Crim. . 9 juill. 1970 - Bull. Crim. 236
[40] Crim. 9 mai 1974 – Gaz. Pal . 1975 . I . 66
[41] Crim. 3 mai 1982 – Bull. Crim. n° 110
[42] Crim. 22 janv 1948 – Bull. Crim. n°26
[43] cf supra

A. L'ATTEINTE AUX DONNEES

Le projet de code pénal envisageait une incrimination unique qui consistait dans le fait de " *intentionnellement et au mépris des droits d'autrui, de détruire ou d'altérer tout ou partie d'un système de traitement automatique d'informations ou d'en entraver ou fausser le fonctionnement* " et qui devait être punie de 5 ans d'emprisonnement et de 2 500 000 F d'amende (l'importance de cette amende révèle combien la fraude informatique peut être une infraction financière).

Mais dès les premières lectures, l'incrimination fut dédoublée en atteinte aux données et atteinte aux systèmes, et l'on revint aux incriminations de la loi Godfrain.

I. ETUDE DE L'ATTEINTE AUX DONNEES

1. Les incriminations

Les articles incriminant les atteintes aux données contenues dans un traitement automatisé de données sont les art. 323-1 et 323-3 CP

L'art. 323-1 sanctionne l'atteinte aux données en tant que ***circonstance aggravante*** : cet article énonce que " *la suppression ou la modification de données contenues dans le système* " est une circonstance aggravante de l'accès ou du maintien frauduleux dans un système de traitement automatisé de données. Elle est punie de 2 ans d'emprisonnement et de 200 000 F d'amende.

L'art. 323-3 érige en ***infraction autonome*** " *le fait d'introduire frauduleusement des données .. ou de supprimer ou de modifier frauduleusement les données .. est puni de 3 ans d'emprisonnement et de 300 000 F d'amende* "

Il peut paraître curieux que ces comportements identiques soient punis de peines différentes, et surtout que la première attitude, précédée d'un accès frauduleux ou d'un maintien frauduleux soit puni moins sévèrement que la seconde. Cela s'explique par le fait dans l'art. 323-1, si l'accès ou le maintien est frauduleux, la conséquence sur les données est involontaire.

2. L'évolution de l'art. 323-3 CP

Il est intéressant d'étudier l'évolution de l'incrimination d'atteinte frauduleuse aux données.

A l'origine, la loi Godfrain avait introduit dans le code pénal l'art. 462-4 qui énonçait que " *Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni ...* "

Nous avons vu que le projet de code pénal modifiait totalement la physionomie de l'arsenal anti-fraude informatique. Le Sénat demanda à revenir à l'incrimination initiale, en en modifiant quelques formules. Ainsi, on supprima la référence " aux mépris des droits d'autrui " pour la remplacer par celle de " frauduleusement ". Par contre, le caractère intentionnel de l'acte était toujours exigé par le rapporteur M. Thyraud pour éviter d'incriminer les actes d'imprudence. De plus, le Sénat supprima l'expression " directement ou indirectement " en considérant qu'il étaient superflus. Il est important de souligner cet épisode législatif car il démontre que la volonté du législateur est d'incriminer par ce texte aussi bien celui qui agit par lui-même, que celui qui agit par l'intermédiaire d'un tiers[44]. Si l'on s'en tient à la volonté du législateur, cela signifie que cet article incriminerait en tant qu'auteur le donneur d'ordre, qui est en droit commun (prévu par l'art. 121-7 CP) considéré comme un complice.

L'Assemblée Nationale acheva la modification de l'incrimination en supprimant l'adverbe " intentionnellement " devenu superflu du fait de la référence au caractère frauduleux de l'acte, ainsi qu'en supprimant la référence au mode de traitement ou de transmission en raison des critiques formulées par la doctrine sur cette formule[45].

[44] débats parlementaires devant le Sénat J.O. du Sénat 30 oct 1991 p.3422 intervention de M. Thyraud
[45] Rapport de la Commission de l'Assemblée Nationale n°2468 12 déc. 1991

3. Une difficulté : le concours d'infractions

Ces atteintes aux données informatiques peuvent concerner des données présentant un caractère de secret défense nationale. Or les articles 413-10 et 413-11 CP incrimine spécialement la destruction de ces données (ils incriminent aussi le détournement mais le sens de cette action paraît floue : il ne peut pas viser le fait de " s'approprier " l'information dans la mesure où la soustraction et la reproduction sont spécialement incriminées. Peut-être cela pourrait-il viser la modification ?).
Il y a alors concours idéal d'infractions. On devra donc poursuivre du chef d'atteinte au secret défense nationale puisque celui-ci est puni plus sévèrement (5 ans d'emprisonnement pour un tiers au secret et 7 ans pour le dépositaire du secret). Mais peut-être peut-on poursuivre pour les deux infractions dans la mesure où ces incriminations protègent des intérêts différents.

II. RAPPROCHEMENT AVEC L'ATTEINTE AUX SYSTEMES

1. L'intérêt de ces incriminations

L'atteinte aux systèmes est très proche de l'atteinte aux données. A tel point que le projet de code pénal voulait, comme nous l'avons vu, incriminer les deux comportements dans un même article en ne faisant référence qu'à l'atteinte aux systèmes.
Il est vrai que l'on peut, en portant atteinte au système atteindre les données par voie de conséquence. Par exemple, introduire un virus qui efface des fichiers porte atteinte à la fois au système et aux données qu'il contient. D'ailleurs, introduire un virus est constitutif de l'introduction frauduleuse de données.
Mais il était bon de distinguer les deux comportements car on peut atteindre les systèmes sans porter atteinte aux données et inversement. Par exemple :
- si l'on s'introduit sur un site web pour y ajouter une photographie, on introduit frauduleusement une donnée dans le système, mais on ne porte pas atteinte au système en lui-même.
- bloquer l'accès à la boîte à lettres électronique d'un internaute en lui envoyant des *spams* ne constitue pas une atteinte aux données : certes, il y a introduction de nouvelles données, mais cela n'est pas frauduleux dans la mesure où c'est la fonction du courrier électronique. Par contre, on peut penser qu'il y a atteinte au système[46].

2. Les incriminations

Ces incriminations ont la même structure que celles d'atteinte aux données :

L'art. 323-1 prévoit une ***circonstance aggravante***. L'altération du fonctionnement du système constitue une circonstance aggravante de l'accès ou du maintien frauduleux

L'art. 323-2 sanctionne une infraction autonome qui est constituée par " *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé des données est puni de 3 ans d'emprisonnement et de 300 000 F d'amende* "

Les remarques faites en matière d'atteinte aux données en ce qui concerne le caractère involontaire des conséquences prévues par l'art. 323-1 sont valables en matière d'atteinte aux systèmes.
Nous pouvons faire deux autres remarques : Tout d'abord, il est intéressant de noter que l'infraction prévue par l'art. 323-2 est punie de 3 ans d'emprisonnement et de 300 000 F d'amende alors que le projet de code pénal prévoyait 5 ans d'emprisonnement et surtout 2 500 000 F d'amende ! De plus, on note une différence de vocabulaire entre l'art. 323-1 et l'art. 323-2 : le premier fait référence à une altération tandis que le second incrimine le fait d'entraver ou de fausser.

3. L'étude particulière de l'art. 323-2

[46] En ce qui concerne les *spams*, les USA partent en croisade contre cette technique : des projets de loi les interdisant sont envisagés, des procès sont engagés et condamnent ces intrusions (informations mai 98 http://www.legalis.net)

L'entrave est connue du droit pénal, notamment grâce au droit pénal du travail. Ici, elle semble avoir le sens d'un empêchement, d'un frein, d'une gêne, d'un obstacle[47]. Le fait de fausser constituerait à détruire et à rendre faux, à changer de signification.
Il faut souligner que selon G. Champy , il ressort des travaux parlementaires de la loi Godfrain que l'altération est un changement de nature et de ce fait un aspect du " faussement ".
Cette conception a l'inconvénient de limiter la portée de l'art. 323-1 : si " faussement " et entrave ne sont pas synonymes et si l'art.323-1 ne réprime que l'altération, forme de " faussement ", cela signifie que la circonstance aggravante de l'art.323-1 ne s'appliquera pas à celui qui entrave involontairement le fonctionnement d'un système après s'y être introduit ou maintenu frauduleusement.

B. LE FAUX ET L'USAGE DE FAUX

La loi Godfrain avait introduit dans le code pénal l'incrimination de faux documents informatisés par l'art. 462-5 et de leur utilisation par l'art. 462-6. Etant donné que ce comportement constitue en fait une modification ou un ajout de données, l'Assemblé Nationale avait voulu n'en faire qu'une circonstance aggravante de l'atteinte aux données. Finalement, une incrimination autonome fut quand même créée.
En première lecture, le Sénat réintroduisit l'incrimination de faux telle qu'elle existait sous l'empire du code de 1810.

Or, le faux " de droit commun " faisant l'objet d'une nouvelle définition extrêmement large, les députés estimèrent qu'un texte spécifique à l'informatique n'était pas nécessaire. En effet, l'art. 441-1 CP considère que " *constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de 3 ans d'emprisonnement et de 300 000 F d'amende* "
Nous remarquons que les peines encourues sont identiques qu'en matière d'atteinte aux données. Cela est sans doute regrettable car il serait logique de sanctionner plus sévèrement celui qui modifier des données dans le but de provoquer des conséquences juridiques que celui qui les modifie " uniquement " frauduleusement.
Mais les circonstances aggravantes relatives aux faux sont applicables et entraînent une sanction plus lourde.

On peut craindre que le problème du faux se développe avec l'utilisation des réseaux par l'Administration. On voit déjà certaines administration travailler via Internet. Ainsi, à Issy les Moulineaux, on peut " commander " ses fiches d'état-civil en envoyant les renseignements nécessaires par courrier électronique[48]. Pour l'instant, ces documents doivent être cherchés à la mairie, mais bientôt ils seront transmis par le même procédé. La Commission européenne favorise elle-même cet essor des documents administratifs disponibles sur le réseau par son action en faveur de la reconnaissance de la validité des signatures numériques[49].

Le développement de la monnaie électronique constitue également une difficulté en la matière. Il se pose la question de savoir si l'incrimination de contrefaçon ou de falsification de monnaie, prévue par l'art. 442-1 CP trouvera à s'appliquer lorsque les délinquants parvient à créer de la monnaie électronique qui n'existe pas. Si ce n'est pas le cas, le délinquant ne sera poursuivi que sur le fondement de l'atteinte aux traitements automatisés de données. L'enjeu de cette discussion est la gravité de la peine encourue car la falsification de monnaie est un crime puni de 30 ans de réclusion criminelle et de 3 000 000 F d'amende.

[47] *La fraude informatique* G. Champy éd. Presses universitaires d'Aix-Marseille 1992
[48] Le Monde 22 nov. 1997
[49] Communication de la Commission " Assurer la sécurité et la confiance dans la communication électronique " COM(97) 503 final

TITRE TROISIÈME. LA MISE EN ŒUVRE DE LA REPRESSION

Après avoir étudié quels sont les comportements susceptibles de s'exprimer par ou sur Internet, ainsi que les sanctions que le droit pénal y attache, nous devons nous interroger dans ce titre second sur la mise en œuvre de cette répression.

Les incriminations étudiées n'ont pas été spécifiquement créées pour appréhender les comportements répréhensibles des internautes ; certaines dispositions sont issues du Code Pénal de 1810 ou d'autres textes anciens. Les juridictions doivent apprécier si ces dispositions sont applicables à ces agissements d'une nature nouvelle et qui vont évoluer. Sans doute, les solutions anciennes ne sont-elles pas transposables à cette nouvelle délinquance et faut-il adapter notre droit afin de mieux la limiter.

Nous étudierons la mise en œuvre de la répression de la " cyber-délinquance " à l'heure actuelle (Chap. I.) avant de s'interroger sur les moyens qui nous permettraient de l'améliorer (Chap.II).

CHAP. I. LES PREMISCES DU DROIT DE L'INTERNET

Depuis quelques années, les juridictions prennent conscience que l'Internet implique une nouvelle forme de délinquance et fait apparaître sous de nouvelles formes des infractions fort anciennes. Nous allons étudier l'attitude des tribunaux face à cette délinquance (Sect°I.) puis les difficultés qu'ils ont rencontrées en mettant en œuvre la répression (Sect°II.).

SECT°. I. LE BILAN JURISPRUDENTIEL

Les juridictions commencent timidement à s'intéresser aux infractions liées à Internet et découvrent peu à peu que notre 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 (§1) et de dégager quelques règles (§2).

§1. LES INFRACTIONS POURSUIVIES

La matière étant récente, la plupart des affaires n'en sont qu'au stade des poursuites (A.). Mais quelques condamnations ont déjà été prononcées (B.).

A. LE STADE DES POURSUITES

I. LE PROXENETISME

En février 1998, un réseau de prostitution ainsi que ses proxénètes a été appréhendé par la police grâce à la dénonciation de l'une des prostituées. Celles-ci rencontraient leurs clients par Internet.

II. LA PUBLICITE

L'application de la loi Toubon a été soulevée dans une affaire récente. Des associations de défense de la langue française avaient porté plainte sur le fondement de la loi n° 97-665 du 4 août 1994 relative à l'emploi de la langue française contre l'Institut de technologie de Géorgie. En effet, son site web, particulièrement destiné à la promotion de cette école auprès des Européens, était rédigé en anglais ce qui semblait violer l'art. 2 de la loi visée qui dispose que toute offre de produits ou de services ainsi que toute publicité écrite, parlée ou audiovisuelle doit être faite en français. Le tribunal de police de Paris, le 9 juin 1997[1], ne trancha pas la question car il débouta les associations pour vices de forme.

Les demandeurs ont fait appel, nous assisterons donc peut-être à l'application de la loi Toubon, même si depuis, les défendeurs diffusent leurs informations en anglais, français et allemand.

III. LE " RACISME "

Avec la pédophilie, le racisme et le révisionnisme sont les dangers d'Internet les plus souvent mis en exergue[2].

Un jugement du TGI de Paris donne un exemple des poursuites pénales qui pourraient être exercées. L'UEJF assignait devant le tribunal civil un auteur-compositeur-interprète et son fournisseur d'hébergement pour avoir diffusé sur un site web des chansons à caractère racistes. Le TGI de Paris, le 10 juillet 1997[3] ne put que déclarer nulle l'assignation des demandeurs en raison du non-respect d'une disposition procédurale de la loi de 1881 : les demandeurs n'avaient pas indiqué la qualification juridique des faits reprochés aux défendeurs, ni le texte applicable. Le tribunal souligne tout de même que les propose du chanteur étaient " *susceptibles de constituer les délits de provocation et injure prévus par les art. 24 al. 6 et 33 al. 3 de la loi du 29 juillet 1881* ".

D'autres poursuites donneront peut-être l'occasion de condamnations pénales : Robert Faurisson a été mis en examen pour contestation de crimes contre l'Humanité[4] pour avoir diffusé sur un site révisionniste un texte dans lequel il affirme que " *l'Holocauste des juifs est une fiction* ". La " tête pensante " d'un réseau néonazi qui exprimait ses idées sur des sites est également mis en examen pour provocation à la haine raciale, apologie de crimes de guerre et de crimes contre l'Humanité[5] (il faut encore que la Grande-Bretagne accepte son extradition).

B. LE STADE DES CONDAMNATIONS

I. LA CONTREFAÇON

L'on voit naître la jurisprudence relative aux infractions commises via Internet essentiellement grâce à des contentieux en matière de contrefaçon. Des organismes comme l'Agence de Protection des Programmes (APP) et son directeur M. Daniel Duthil se sont lancés dans la lutte contre la contrefaçon sur Internet et agissent avec beaucoup de pugnacité.

Les ordonnances de référé ayant statué en la matière ont confirmé que les notions de reproduction et de représentation de l'œuvre, pour lesquelles le copiste doit obtenir l'accord du titulaire des droits sur l'œuvre, sont applicables à la mise en ligne d'une œuvre.

---

[1] Trib. Police Paris 9 juin 1997 Ass° Défense de la langue française, Avenir de la langue française c/ Ass° Georgia Tech Lorraine – " au fil du Net " Gaz. Pal. 10, 12 août 1997 p.25 - Gaz. Pal. 19, 21 oct. 1997 som. P.41

[2] Pour s'en rendre compte par soi-même : http://www.abbc.com/aaargh/ - http://abbc.com/islam/french/textes/

[3] TGI Paris 10 juill. 1997 – Gaz. Pal. 18 , 20 janv. 1998 p.42 – http://www.aui.fr

[4] " Robert Faurisson mis en examen pour contestation de crimes contre l'humanité " Le Monde 19 nov. 1997

[5] " Policiers et gendarmes démantèlent un réseau néonazi qui agissait sur Internet " Le Monde 19 fév 1998

Certains auteurs[6] font remarquer que les juridictions ne qualifie pas l'acte de contrefaçon et se contentent de constater une reproduction et une représentation sans autorisation[7].

1. Le droit de reproduction

Nous avons déjà vu que la reproduction se définie comme " *la fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte* " et qu'elle doit être autorisée par le titulaire des droits sur l'œuvre, excepté dans les cas où elle a pour objet une copie privée ou une courte citation.

a) La reproduction

Les quelques ordonnances rendues en la matière reconnaissent implicitement que la numérisation d'une œuvre puis sa mise en ligne sur un site web[8] ou un site FTP[9] constituent une reproduction.

- Il y a **fixation matérielle** par la numérisation, cette dernière étant définie par le Tribunal de Grande Instance de Paris dans la première affaire Queneau[10] comme la " *technique consistant à traduire le signal analogique qu'elle constitue en un mode numérique ou binaire qui représentera l'information dans un symbole à deux valeurs 0 et 1 dont l'unité et le Bit* ". Le tribunal de grande instance de Paris a reconnu la première fois[11] ce mode de reproduction de façon curieuse : il reconnaît que " *la reproduction par numérisation d'œuvres musicales protégées par le droit d'auteur susceptible d'être mise à la disposition de personnes connectées au réseau Internet doit être autorisée expressément par les titulaires ou cessionnaires des droits* ", mais cette formule est celle que les demandeurs sont autorisés à diffuser et non pas un attendu du tribunal.
- C'est également une fixation qui **permet de communiquer l'œuvre au public**. C'est-à-dire que la copie à usage privé est par contre autorisée. Cette question fut celle sur laquelle les défendeurs se fondaient pour écarter leur responsabilité, notamment dans les litiges qui donnèrent lieu aux ordonnances du 14 août 1996. Les étudiants qui avaient installé sur les pages de leur site web des chansons de Jacques Brel et de Michel Sardou considéraient que les copies qu'ils avaient faites n'étaient destinées qu'à leur propre usage et quelles se situaient sur leur " domicile virtuel ". Le tribunal ne fut pas de cet avis et considéra qu'il ne pouvait pas y a voir copie privée dans la mesure où tout internaute peut se connecter à toute page d'un site web et d'en prendre copie : de ce fait, les défenseurs ont " *favorisé l'utilisation collective de ses reproductions* ". Le tribunal ajoute qu' " *il importe peu qu'il n'effectue (le défendeur) lui-même aucun acte positif d'émission : l'autorisation de prendre copie étant implicitement contenue dans le droit de visiter les pages privées* ". Pour résumer, selon les défendeurs, ils ont un rôle passif et ce sont les internautes qui viennent chercher l'information à leur " domicile " tandis que pour les juridictions, même si les défendeurs n'effectuent aucun acte positif, ils savent que les informations qu'ils stockent sur leur site sont, en raison du fonctionnement du World Wide Web et de la raison de son existence, sont susceptibles d'être appréhendées par tout internaute.

b) La courte citation

Le défendeur dans la première affaire Queneau[12], qui avait mis sur son site web des poèmes de Raymond Queneau, avait invoqué que sa copie constituait une courte citation, qui ne nécessite pas l'autorisation du titulaire des droits sur l'œuvre. Mais le tribunal a rejeté cet argument pour deux raisons.
Tout d'abord, il ne pouvait y avoir courte citation dans la mesure le procédé employé par le défendeur permettait de reconstituer l'intégralité de l'œuvre.
De plus, le tribunal estime que les pages du site sur lequel il avait mis en ligne les poèmes ne constituaient pas des documents à but critique, polémique, pédagogique, scientifique ou d'information, seuls domaines pour lesquels une courte citation est tolérable selon l'art. L.122-5 CPI.

2. Le droit de représentation

[6] " Contrefaçon et droit d'auteur sur Internet (1ère partie) " L. Tellier-Loniewski, C. Rojinsky, L. Masson – Gaz. Pal 19,21 oct. 1997 p.20
[7] Les ordonnances de référé du TGI de Paris du 14 août 1996 dans les affaires Sardou et Brel font quand même référence à " l'allégation de contrefaçon ".
[8] TGI Paris 14 août 1996 affaires Sardou et Brel – TGI Paris 5 mai 1997 affaire Queneau
[9] TCom. Paris 3 mars 1997
[10] TGI Paris 5 mai 1997 – JCP 1997 éd. G. II. 22906
[11] TGI Paris 14 août 1996 affaires Sardou et Brel
[12] ord. Réf. TGI Paris 5 mai 1997

La représentation se définie comme " *la communication de l'œuvre au public par un procédé quelconque, et notamment, par récitation publique, exécution lyrique../..par télédiffusion* ".

L'atteinte au droit de représentation n'est pas directement visée par les juridictions qui ont eu à statuer sur des contentieux relatifs à la contrefaçon. Cela se justifie dans la mesure où les contentieux ont fait apparaître des reproductions qui impliquent la possibilité d'une représentation.

Certains auteurs[13] estiment que l'ordonnance de référé rendue le 3 mars 1997 par le tribunal de commerce de Paris[14] reconnaît expressément que le droit de représentation était également violé lors de la mise à disposition d'un logiciel sur Internet. Il faut sans doute rester nuancé car l'ordonnance n'indique pas en quoi ce droit aurait été atteint et ne fait référence au droit de représentation que lorsqu'elle interdit au défendeur de " *distribuer toute reproduction et/ou représentation totale ou partielle du logiciel* ".

Il faut souligner que les juridictions ont statué sur des espèces où les copies étaient mises en ligne sur des Sites web ou FTP. La question demeure lorsque la copie est mise en ligne sur un service tel que le courrier électronique[15].

A priori, l'exception de copie privée pourrait être retenue.

Mais parfois, le courrier électronique fait l'objet d'une diffusion massive, notamment dans le cadre des listes de diffusion. Dans cette hypothèse, l'argument de la copie privée ne pourrait plus être retenu, d'autant plus que les défendeurs ne pourraient pas cette fois-ci invoquer l'absence d'acte positif de leur part.

II. LA PROTECTION DE LA PERSONNE

1. Les données personnelles

La première décision en matière de protection de la représentation de la personne a été rendue par le tribunal correctionnel de Privas en septembre 1997[16].

Un jeune homme, vexé d'avoir été quitté par son amie, avait piraté le site Internet d'une municipalité ardéchoise pour y installer des photographies pornographiques de la jeune fille, photographies ""*complétées" par un texte en relation avec celles-ci quant aux mœurs de la personne représentée* " pour reprendre la formule du tribunal. Notons qu'il avait également doté la photographie du maire de la commune de cornes, mais aucune poursuites sur ce chef ne furent engagées, ce qui est quasiment toujours le cas (on demande simplement aux pirates de retirer leurs " œuvres ").

Il fut poursuivi et condamné sur le fondement de l'art. 226-19 CP, c'est à dire pour avoir mis ou conservé en mémoire informatique des données nominatives sans l'accord exprès de l'intéressée qui directement ou indirectement faisaient apparaître ses mœurs.

Le tribunal adopte le parti de condamner sur le fondement de la mise en mémoire. On peut penser qu'il aurait pu choisir de poursuivre et de condamner sur le fondement de l'art.226-2 CP qui sanctionne le fait porter ou de laisser porter à la connaissance du public ou d'un tiers l'image d'une personne se trouvant dans un lieu privé. Cependant, nous pensons que l'action n'aurait pas prospérer car deux difficultés l'en aurait empêché.

- Les peines de l'art. 226-2 CP sont beaucoup moins importantes que celles de l'art. 226-19 (1 an d'emprisonnement et 300 000 F d'amende contre 5 ans d'emprisonnement et 2 000 000 F d'amende). Si l'option de l'art. 226-2 avait été choisie, soit l'art. 226-19 n'aurait pas été utilisé alors que cela pourra s'avérer utile dans des affaires graves, soit l'art. 226-19 aurait appliqué par d'autres juridictions, ce qui aurait entraîné des différences d'une juridiction à une autre.
- L'application de l'art. 226-2 se heurte à une grande difficulté. Nous avons vu dans le premier chapitre qu'il n'était pas nécessaire que celui qui diffuse la photographie ait l'intention de porter atteinte à l'intimité de la vie privée de la personne représentée, mais que par contre, il fallait que la photographie ait été prise initialement sans le consentement de la personne et dans le but de porter atteinte à l'intimité de la vie privée de celle-ci. Dans l'espèce étudiée, une discussion aurait du avoir lieu sur le caractère attentatoire des photographies. Or il y a de fortes chances pour que la jeune fille ait accepté d'être prise en photo. Le jeune homme aurait alors été relaxé.

---

[13] " Contrefaçon et droit d'auteur sur Internet (1ère partie) " L. Tellier-Loniewski, C. Rojinsky, L. Masson – Gaz. Pal 19,21 oct. 1997 p.20

[14] JCP 1997 éd.G . II. 22840

[15] " Contrefaçon et droit d'auteur sur Internet (1ère partie) " L. Tellier-Loniewski, C. Rojinsky, L. Masson Gaz. Pal 19,21 oct. 1997 p.20 - " Internet et la loi " T. Piette-Coudol & A. Bertrand coll. Dalloz service éd. Dalloz 1996 p.146

[16] Trib. Privas 4 sept. 1997 http://www.legalis.net/legalnet

Nous nous rendons donc que ce jugement, s'il faisait jurisprudence, conférerait une protection plus grande aux représentations de la personne dès lors qu'elles seraient divulguées par un support informatique (plutôt que par un autre support).

2. La diffamation

Les quelques décisions en la matière sont des ordonnances de référé.

La principale est celle rendue par le TGI de Paris le 30 avril 1997[17] : le journal l'Express avait consacré un article à l'ESIG intitulé " Carambouille à l'école ", expliquant que le directeur de l'école se livrait à des détournements et escroqueries. Cet article avait été reproduit sur le site web du journal et le directeur visé, après avoir fait condamner le journal pour l'article papier tentait de faire condamner le journal pour l'article diffusé sur Internet.
Le tribunal reconnu que la loi de 1881 était applicable à Internet : " *la diffusion de tels propos sur le réseau Internet, à destination d'un nombre indéterminé de personnes nullement liées par une communauté d'intérêts, constitue un acte de publicité distinct de celle résultant de la mise en vente du journal l'Express et commis dès que l'information a été mise à la disposition des éventuels utilisateurs du site* ".
L'action civile en diffamation ne fut cependant pas étudiée quant au fond car, en application de la loi de 1881, le délai de prescription de 3 mois était acquis. Il est tout de même important de remarquer que le tribunal considère que même en matière d'Internet, le point de départ du délai de prescription est le jour de la première diffusion de l'information litigieuse et non le jour où les faits ont été constatés.

3. Les menaces

Un tribunal correctionnel a reconnu les dispositions de l'art. 222-7 CP à un message diffusé sur Internet. Un propriétaire de pitbulls contestant l'action du député A. Santini en faveur de la disparition de cette race de chiens et lui ayant pour cette raison adressé des menaces de mort via le site web du parlementaire, a été condamné à 2 mois d'emprisonnement avec sursis.[18].

III. LA " PEDOPHILIE "

Les autorités judiciaires ont également pris conscience de la gravité de ces faits.

Dans un premier temps, les gérants de deux serveurs d'hébergement et fournisseurs d'accès, WorldNet et FranceNet ont été mis en examen le 7 mai 1996 pour diffusion et transmission d'images pornographiques de mineurs. L'information n'est pas close, mais le procès s'avère d'ores et déjà intéressant car les gérants contestent que leur responsabilité pénale puisse être engagée[19].

Des poursuites sont également en cours à l'encontre de personnes échangeant des images pornographiques de mineurs sur le réseau. Les opérations les plus médiatiques sont l'*opération Achille* et *l'opération Cathédrale*. La première[20], menée en décembre 1997 a abouti à la mise en garde à vue d'une cinquantaine de personnes dont cinq furent mises en examen pour diffusion et recel d'images de mineurs à caractère pornographique. Les enquêteurs avaient retracé le parcours des internautes et identifié les utilisateurs français. L'enquête avait été diligentée à la suite d'une plainte d'une association de défense et de protection de l'enfance. La seconde[21] a permis, grâce à une étroite collaboration des polices de 21 pays , l'arrestation d'une centaine de personnes et la saisie de plus d'une centaine de milliers de photographies.

---

[17] TGI Paris ord. Réf. 30 avril 1997 sté ESIG, Roger B. c/ sté Groupe Express http://www.legalis.net/legalnet – Gaz. Pal. 1997 som. P.41

[18] jugement du 28 avril 1998 – http://www.legalis.net – solutions identiques par des juridictions étrangères : condamnation d'un Danois à une amende de 2 000 couronnes pour avoir envoyé des menaces de mort à un journaliste via Internet (Le Monde 2 sept 1998) ;condamnation à un an d'emprisonnement d'un étudiant américain ayant menacé de mort d'autres étudiants (informations de mai 98 http://www.legalis.net)

[19] voir le communiqué de FranceNet du 13 mai 1996 à ce sujet " Comment devenir pédophile en 24h " http://www.francenet.fr/comment/comment.html

[20] " Des internautes interpellés pour échanges d'images pédophiles " Le Monde 11 déc. 1997

[21] " Un vaste réseau de pédophiles opérant sur Internet a été démantelé par les polices de 21 pays " Le Monde 4 sept 1998

Jusqu'à récemment, seules quelques juridictions étrangères avaient condamné ces agissements. Ainsi, un étudiant danois a été condamné en septembre 1997 a une amende de 2 000 F pour propagation d'images pornographiques enfantines[22]. Il avait en effet diffusé sur Internet 3 121 images pornographiques dont 533 de rapports sexuels entre des enfants et des adultes ou des animaux (on nous précise que le tribunal s'est montré clément car il n'avait pas l'intention de vendre ces photos mais uniquement de les échanger, un peu comme un collectionneur de timbres selon la formule de son avocat !). De même, une américaine fut condamnée par un tribunal suisse pour avoir envoyé dans ce pays des photos pédophiles à un ami via Internet. Les juridictions américaines ont également prononcé des condamnations[23].

La première condamnation française a été prononcée par le tribunal correctionnel du Mans le 16 février 1998[24] à l'encontre du directeur de Cabinet du Président du Conseil Général de la Sarthe. Celui-ci utilisait l'ordinateur du secrétariat afin de se connecter à Internet, ce qui lui avait permis de recevoir un millier d'images pornographiques de mineurs.

Le jugement n'est pas clair quant au fondement de la condamnation : s'il est certain que le prévenu est condamné pour recel d'images obtenues à l'aide de l'infraction d'enregistrement ou diffusion d'images pornographiques de mineur (art. 227-23 CP), mais certains passages du jugement laissent entendre qu'il est également condamné pour recel d'images pornographiques obtenues à l'aide de l'infraction de corruption de mineur (art. 227-22 CP). De plus, le Parquet du Mans envisagerait de poursuivre le fournisseur d'accès sur le fondement du transport ou diffusion d'un message à caractère pornographique susceptible d'être perçu par un mineur (art. 227-24 CP) ou de la complicité du recel.

§2. LES REGLES DEGAGEES

De ces quelques jugements, se dégagent des remarques relatives aux sanctions prononcées (A.)et aux règles de compétence suivies (B.).

A. DES SANCTIONS APPROPRIEES

Les sanctions sont rares dans la mesure où les poursuites sont peu nombreuses. Ainsi, en matière de piratages de sites web, pourtant très nombreux, les infractions sont classées sans suite après que les pirates ont rendu leur apparence normale aux sites.

Toutefois, certaines sanctions ont déjà été prononcées[25]. Un jeune homme a été condamné à soixante heures de travail d'intérêt général pour avoir introduit un logiciel permettant de rapatrier sur son ordinateur les mots de passe des utilisateurs d'un réseau[26]. Le jeune homme poursuivi à Privas pour avoir mis en mémoire informatique des données nominatives laissant apparaître les mœurs de la victime[27] a été condamné à huit mois d'emprisonnement avec sursis et à 5 000 F d'amende. A l'encontre du premier condamné pour recel de photos pédophiles[28] a été prononcé six mois d'emprisonnement dont trois avec sursis.

Mais il semble que des sanctions originales, liées à la spécificité du réseau voient le jour.

C'est en matière de contrefaçon qu'ont été dégagées les premières solutions originales en matière de sanctions. Certes, le peu de décisions innovantes en la matière émane de tribunaux de grande instance ou de tribunaux de Commerce statuant en référé. Les dispositions prises par ces juridictions ne sont pas des sanctions,

---

[22] Dépâche AFP 25 sept. 1997

[23] http://pedowatch.org/index-f.htm : 14/05/97 : 30 ans d'emprisonnement pour un membre d'un club de pornographie infantile – 23/06/97 :10 ans d'emprisonnement pour un homme qui avait contacté une jeune fille de 13 ans sur une messagerie en-ligne, puis par téléphone et par courrier, et qui lui demandait de lui envoyer des photos et vidéos d'elle dans des positions sexuelles…

[24] TCorr. Le Mans – 16 fév 1998 – http://www.legalis.net – Expertises mars 1998 (http://www.celog.fr)
Ce jugement est également intéressant dans la mesure où il condamne de plus le prévenu pour abus de confiance en raison de l'utilisation détournée qu'il a fait " d'un micro-ordinateur et un disque dur " qui lui avaient été remis pour un usage professionnel. Ce jugement va donc à l'encontre de la partie de la doctrine (F. Chamoux JCP 1988.I.3321) qui estime que le " vol de temps-machine " est constitutive de l'accès frauduleux incriminé par l'art. 323-1 CP.

[25] Par exemple à l'étranger, un tribunal des Emirats arabes unis a condamné en sept. 1997 quatre étrangers à 6 mois à un an d'emprisonnement pour avoir piraté des lignes d'abonnés d'Internet. Dépêche AFP 30 sept. 1997

[26] " Cyberwars : la montée du crime informatique " Les Echos 10 fev 1998 p.55

[27] Trib. Corr. Privas 4 sept. 1997

[28] Trib. Corr Le Mans 16 fév. 1998

mais des " mesures conservatoires ou de remise en état "[29]. Elles annoncent cependant ce que pourraient être les sanctions de demain en matière d'infractions commises via Internet.

L'ordonnance de référé rendue par le Tribunal de Commerce de Paris le 3 mars 1997[30] ose innover. Une société avait mis en ligne sans autorisation de son auteur, sur un site FTP des contrefaçons d'un logiciel, régulièrement déposé auprès de l'APP. Cette mise en ligne permettait à tout internaute de télécharger gratuitement ce logiciel.
Le Tribunal de Commerce fait droit aux demandes proposées par la demanderesse, c'est-à-dire trois types de mesures.

→ l'interdiction sous astreinte journalière de distribuer le logiciel.

→ la publication sur la page d'accueil du site de la condamnation.

Ce type de mesure est classique, elle est prévue par de nombreux textes (contrefaçon art. L. 335-6 CPI – comme peine complémentaire art. 131-10 & 131-35 CP), et peut constituer une sanction. Elle vise le " rétablissement moral de la victime "[31]. Cette publication est garantie par la condamnation à une astreinte journalière en cas de non-respect (de 10 000 F). Elle est ordonnée pour une durée de 6 mois. Comme le fait remarquer M. Gautier, cette limitation dans le temps de la mesure se retrouve dans toute sanction pénale, durée après laquelle " *le site ayant en quelque sorte " purgé sa peine " reprendra sa liberté* ".

Différentes remarques s'imposent à propos de cette mesure.

- Le tribunal de Commerce apporte une précision quant au contenu de la publicité. Son texte devra être établi entre les parties.
- Le tribunal de Commerce impose que la publicité figure sur la page d'accueil du site. Cette mesure a pour objet d'assurer que la publicité soit connue d'un maximum d'utilisateurs puisque chaque connexion à un site implique de visualiser ce qu'on appelle le " home page ". Mais quelques difficultés peuvent être soulevées.

La première page d'un site est, quasiment comme toutes les pages d'un site, d'une longueur plus importante que celle de l'écran du moniteur. Elle se présente en effet comme une page déroulante, dont l'internaute ne fait pas, en général, défiler l'intégralité. Il se peut donc qu'en créant un " home page " d'une longueur légèrement importante, la publicité ne soit pas lue. De plus, il se peut que les serveurs condamnés essayeront de limiter la portée de la publicité en ne prévoyant sur la page d'accueil qu'un lien hypertexte avec une autre page reproduisant la condamnation. La jurisprudence aurait alors à décider si l'existence d'un intitulé du type " texte des décisions de condamnations à l'encontre de notre serveur " figurant en langage HTML constituerait une publicité suffisante.

- Nous avons déjà souligné que cette condamnation n'était qu'une mesure ordonnée en référé et non une sanction pénale. Une telle sanction pénale serait-elle imaginable dans la mesure où le juge ne peut pas prononcer de sanction qui ne soit pas prévue par la loi ? L'art. 131-35 CP prévoit que " *la diffusion de la décision est faite par le Journal Officiel de la République Française, par une ou plusieurs autres publications de presse, ou par un ou plusieurs services de communication audiovisuelle.* " Prononcer comme sanction pénale la diffusion de la condamnation sur la page d'accueil d'un site web ne sera donc possible que dans la mesure où ce type de service sera reconnu comme un service de communication audiovisuel.

→La création d'un lien hypertexte entre la première page du site poursuivi et le site de l'APP.

L'originalité de cette mesure est d'emprunter à la technique d'Internet. En principe, les liens entre sites sont décidés d'un accord commun entre les serveurs. Ce type de mesure trouvera à être prononcée dans beaucoup d'autres hypothèses : le serveur diffusant des propos racistes pourra se voir imposer de créer un lien avec un site d'association de défense des droits de l'Homme, celui diffusant des messages présentant la consommation de stupéfiants sous un jour favorable, un lien avec le site d'un hôpital…
Il demeure que jusqu'à présent, aucune sanction pénale de la sorte n'a été prononcée et ne peut pas l'être tant que le législateur ne prévoit pas une telle sanction.

B. UNE COMPETENCE ETENDUE

[29] art. 809, 849 & 873 CPCiv.
[30] JCP 1997. II. 22840 note F. Olivier & R. Barbry – " Première affaire en matière de contrefaçon en matière de logiciel sur l'Internet " http://www.legalis.net – " Suite de la promenade à travers un site immatériel : des condamnations en nature sur l'Internet " P.-Y. Gautier D. 1997 chron. P. 176
[31] " Suite de la promenade à travers un site immatériel : des condamnations en nature sur l'Internet " P.-Y. Gautier D. 1997 chron. P. 176

Comme en matière de sanctions, le bilan des règles dégagées en matière de compétence territoriale est délicat car la plupart des décisions sont rendues suivant la procédure de référé et dans des contentieux qui reconnaissent des règles particulières de compétence.

En matière de contrefaçon, les défendeurs lors de la seconde affaire Queneau [32], avaient soulevé l'incompétence du tribunal de grande instance de Paris en invoquant que le serveur d'hébergement défendeur à l'action se trouvait dans le ressort du TGI de Toulouse. Selon la jurisprudence classique en matière de contrefaçon, aussi bien civile que pénale, le TGI de Paris s'est estimé compétent puisque la contrefaçon avait été constatée à Paris.

De la même manière, lors de contentieux relatif à la presse et à l'audiovisuel, les juridictions compétentes sont traditionnellement toutes celles dans le ressort desquelles la diffamation ou autre atteinte a été perçue. C'est ce que rappelle la Cour de Justice des Communautés Européennes dans un arrêt du 7 mars 1995[33]. Le TGI de Paris par une ordonnance de référé du 16 avril 1996[34] s'était ainsi déclaré compétent car les propos diffamatoires diffusés sur Internet étaient " *accessibles..pour tout intéressé à Paris* ".

Ces solutions énoncées par des ordonnances de référé pourraient être confirmées en matière pénale par des tribunaux correctionnels.

Le tribunal correctionnel de Privas dans son jugement du 4 septembre 1997 n'aborde qu'implicitement la question. Selon le Ministère Public, le prévenu est poursuivi pour avoir mis ou conservé en mémoire informatique des données nominatives sensibles " *à Talencieux et sur l'ensemble du territoire national* ".La référence à Talencieux permet sans doute de justifier la compétence territoriale du tribunal de Privas. La formule *" et sur l'ensemble du territoire national "* paraît signifier que toute juridiction française aurait été également compétente. Une telle pluralité de compétence peut se justifier par les articles 382 et 522 CPP Ces derniers énoncent que sont compétents les tribunaux du lieu de l'infraction, de la résidence du prévenu, du lieu d'arrestation du prévenu. De plus, la juridiction compétente pour juger l'un des prévenus est compétente pour juger les autres auteurs ou complices. Il faut alors admettre, comme en matière de presse que les infractions sont réputées commises dans tous les lieux où elles sont accessibles. Le tribunal ne s'est pas interrogé sur ce point, tout au plus a-t-il restreint la compétence à sa juridiction en ne faisant référence comme lieu de commission qu'à Talencieux.

En pratique, les juridictions distinguant rarement la compétence territoriale de l'application de la loi pénale, cette dernière conditionnera la première.

SECT°. II. 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 (§1) que techniques (§2), qu'elles rencontrent en la matière.

§1. LES DIFFICULTES JURIDIQUES

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

A. L'APPLICATION DE LA LOI PENALE DANS L'ESPACE

[32] TGI Paris ord. Référ. 10 juin 1997 aff. Queneau c/ Jérôme B. , le LAAS
[33] CJCE 7 mars 1995 D.1996. 61
[34] TGI Paris ord. Réf. 16 avril 1996 – D.1997 som.com.p.72

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

I. LES DIFFICULTES

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 a 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-Uni[1]s, 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 de 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.

En droit pénal français, trois principes peuvent être suivis pour déterminer la loi pénale applicable[2].

1. La théorie de l'émission

Cette théorie, encore appelée celle de l'injection, consiste à reconnaître l'application de la législation du pays d'où provient le message incriminé. Ainsi, celui qui diffuse sur un site américain un message à caractère révisionniste ne serait pas inquiété, même si ce site peut être consulté de France par exemple.

Cette théorie a déjà été adoptée dans une autre matière qui implique une diffusion internationale et qui est celle de " la transmission transfrontière et la retransmission de services de programmes de télévision ". En effet, elle fut adoptée par la Directive européenne " Télévision sans frontières " n°89/552/CEE du 3 octobre 1989 et reprise par la nouvelle directive du 30 juin 1997 dans leur article 2-1[3].

Cette solution peut se justifier de trois façons :

- Tout d'abord, elle se justifie dans la mesure où on ne peut pas exiger de l'utilisateur du réseau qu'il connaissance et respecte les législations de tous les Etats de la planète, c'est-à-dire près de 200.
- De plus, elle peut se justifier par l'application de la territorialité en matière de compétence. On pourrait considérer que la prise de connaissance de l'information litigieuse ne se fait non sur le territoire de l'Etat dans lequel réside l'utilisateur, mais sur le territoire de l'Etat d'où est édité le message en estimant que celui qui perçoit le message se " déplace virtuellement " au lieu d'émission. Ce raisonnement pourrait être illustré en matière de casinos virtuels. Nous avons vu que l'organisation en France de jeux de hasard fait l'objet d'une réglementation stricte, dont toute violation constitue une infraction. Or il existe de nombreux sites proposant des jeux de hasard accessibles de France. Beaucoup d'entre eux sont situés dans des Etats américains qui réglementent superficiellement ce type d'activité (il faut noter que ce n'est le cas que de quelques Etats américains). Dès lors, participer à l'un de ses jeux entraînerait un transport virtuel au lieu du serveur. L'activité ne se ferait pas au lieu d'implantation de l'ordinateur du joueur. Seule la loi de l'Etat américain serait applicable et permettrait ainsi l'activité.
- Enfin, certains auteurs[4] soulignent que les différentes législations incriminent les mêmes comportements et ne se distinguent que sur des infractions peu nombreuses. Mais on peut considérer ces dernières (différences d'appréciation quant aux bonnes mœurs, le révisionnisme…) comme suffisamment importantes pour considérer la théorie de l'émission comme imparfaite.

---

[1] ainsi qu'aux Pays-Bas

[2] " Internet, le législateur et le juge " N. Gautraud Gaz. Pal 1996. n°299-300 p61 – " Le droit applicable à Internet : de l'abîme aux sommets " N. Brault http://www.grolier.fr/cyberlex.net – " Cybermonde : Droit et droits des réseaux " M. Vivant JCP 1996 .II.3969 – *Lamy informatique* 1997 n°2132 & s.

[3] art. 2-1 dir. n°97/36/CE du 30 juin 1997 : " *Chaque Etat membre veille à ce que toutes les émissions de radiodiffusion télévisuelle transmises par des organismes de radiodiffusion télévisuelle relevant de sa compétence respectent les règles du droit applicable aux émissions destinées au public dans cet Etat membre* "

[4] "L'Internet et le droit pénal " J.F Chassaing D.1996 n°38 doctr. p.329

MM. Piette-Coudol et Bertrand[5] proposent une solution proche de la théorie de l'émission : la compétence du lieu de " mise à disposition " sur Internet.
Le principe est le même que celui qui gouverne la théorie de l'émission : celui qui émet l'information est soumis à la législation du lieu à partir duquel il agit et ne peut pas être poursuivi en vertu d'une autre législation que celle du lieu de " mise à disposition ". Par contre, celui qui, à partir d'un autre lieu, va chercher l'information et la rapatrie dans le pays où il est situé est soumis à la législation de ce dernier et s'expose à des poursuites s'il en a violé les règles. Cette solution est en fait l'application de la théorie d'émission, la responsabilité de l'utilisateur suivant le régime de droit commun (il sera poursuivi quand il y aura infraction impliquant une détention ou un recel).

L'inconvénient majeur de la théorie de l'émission est de favoriser l'impunité. De la même manière qu'il existe des " paradis fiscaux ", certains Etats apparaîtront comme des " paradis Internet " dans la mesure où leur législation sera relativement souple sur certains comportements. Ainsi, tous les serveurs néo-nazis s'installeront aux Etats-Unis[6] et au Canada, tous les serveurs offrant des services de casino dans les Caraïbes etc..

L'art. 113-6 CP permettrait de limiter un tant soit peu ces effets néfastes. Il permet en effet de poursuivre selon la loi française le ressortissant français qui commet une infraction à l'étranger. Mais nous voyons tout de suite les limites de ce texte. Il faudrait tout d'abord que toutes les législations soient dotées d'un principe d'application de la loi en vertu de la personnalité active pour que tout délinquant soit poursuivi. De plus, si cette disposition tempère l'inconvénient de l'existence de " paradis Internet " en matière de crime, elle est inefficace en matière de délit. En effet, elle exige que les poursuites soient ouvertes à la suite d'une plainte de la victime ou d'une dénonciation officielle et que l'infraction fasse l'objet d'une incrimination dans le pays de sa commission.

2. La théorie de la réception

La théorie de la réception opte pour la conception inverse : le message serait soumis à la législation du pays dans lequel il est reçu.

Cette théorie fut appliquée par un tribunal new-yorkais [7] qui ordonna à un serveur italien de cesser d'utiliser la marque Playmen sur la demande la société diffusant la marque Playboy parce que ce serveur était accessible aux internautes américains. De la même façon, le tribunal de Lausanne condamna une résidente américaine qui avait envoyé des photos pédophiles à un ami suisse[8].

Cette conception a pour avantages de protéger la souveraineté des Etats en matière de justice, d'assurer ainsi la défense de " valeurs essentielles "[9]que la société (française, en l'occurrence) a affirmé, et d'éviter des situations de fraude à la loi favorisée par la conception de l'émission

Ses inconvénients sont également nombreux et rejoignent les avantages de la théorie de l'émission.

- Cette conception porterait atteinte à des principes essentiels du droit pénal français et international : la stricte application de la loi pénale et le principe de légalité des délits et des peines

- En cas de pluralité de poursuites (hypothèse qui se rencontrerait très certainement), les Etats hésiteraient sans doute à abandonner leurs poursuites au profit d'un autre en raison de la méfiance à l'égard des juridictions étrangères et du refus de la moindre atteinte à leur souveraineté. De plus, le principe " non bis in idem " étant rarement respecté de nos jours, il est probable que l'application d'une telle théorie ne ferait qu'accroître son non-respect. Seule une véritable et totale coopération internationale permettrait de surmonter ces obstacles.

- Une difficulté technique peut également s'opposer à cette théorie. Comme l'ont fait remarquer des défendeurs dans des contentieux en matière de contrefaçon[10], l'originalité de certains services d'Internet comme le web est que " *le créateur d'une page web sur le réseau Internet n'accomplit aucun acte positif d'émission à l'égard des autres utilisateurs du réseau mais, au contraire, ce sont les autres utilisateurs qui vont chercher l'information* ". Si on s'en tient à cette remarque, fondée techniquement, il est vrai qu'on peut considérer qu'il

[5] *Internet et la loi* T. Piette-Coudol & A. Bertrand coll. Dalloz Service éd. Dalloz 1996 p. 55
[6] le 18 février 1998, les médias annonçaient la fermeture d'un site néo-nazis installé sur un serveur français (et la mise en examen de certains de ses éditeurs) mais aussi que le site avait aussitôt était transféré sur un serveur américain.
[7] Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996) – http://seamless.com/
[8] " Publicité sur Internet : droit et déontologie "N. Varille Gaz. Pal. 21,22 nov. 1997 p.5
[9] " Cybermonde : Droit et droits des réseaux " M. Vivant JCP 1996 II. 3969
[10] TGI Paris 14 août 1996 affaires Sardou et Brel

serait injuste de poursuivre un éditeur dont le message parvient dans un pays sanctionnant ce type de message : l'éditeur n'a pas effectué d'acte positif pour faire parvenir ce message dans ce pays et si le message est y parvenu, c'est du fait de l'action d'un utilisateur situé dans ce pays.
Mais ce raisonnement ne peut être soutenu, dans la mesure où l'essence même du réseau est une communication internationale : aucun éditeur de contenu ne peut ignorer que son message sera susceptible d'être perçu dans tous les pays.

- Par contre, il est impossible pour qui que ce soit de maîtriser et de respecter la législation de 200 Etats souverains et c'est ce qu'impliquerait l'adoption de cette théorie dans la mesure où tout message diffusé sur Internet, et notamment sur le web, est susceptible d'être appréhendé dans tous ces pays.

Si cette théorie devait être adoptée, il pourrait exister deux techniques pour échapper à sa responsabilité pénale.

La première serait d'invoquer l'erreur de droit, du moins dans les pays où elle est reconnue comme cause d'irresponsabilité. Face aux juridictions françaises, celle-ci devrait toujours être inévitable comme le prévoit l'art. 122-3 CP.

On pourrait de plus exiger de l'éditeur qu'il respecte, non pas les législations de tous les Etats, mais du moins les législations des Etats dans lequel son message a vocation à être diffusé, les législations des pays dont il cherche à toucher les habitants (lorsque le public visé est limité). C'est une solution qui pourrait être adoptée en matière d'application de la loi Toubon et que le tribunal de Police de Paris aurait pu adopter s'il avait jugé au fond le contentieux qui lui était présenté le 9 juin 1997[11]. Il demeure que si la question est étudiée sur le fond[12], elle pourrait se résoudre par rapport à la destination de l'offre ou de la publicité. Il est évident qu'on ne peut pas poursuivre tous les sites qui existent pour non-respect des dispositions de la loi Toubon au nom du fait qu'ils sont accessibles de France, cela n'aurait aucun sens, d'autant plus que 90 % des services commerciaux sont en anglais. Par contre, on pourrait peut-être exiger que la loi s'applique à l'égard des sites destinés spécifiquement à être consultés en France[13]. La mise en œuvre d'une telle règle d'application du droit en fonction du public auquel est destiné le message pourrait être facilitée (et jouer en la faveur des annonceurs) si les annonceurs de publicités notamment décidaient de désigner les cibles auxquelles ils s'adressent au moyen d'un " drapeau "[14].

3. La théorie de l'ubiquité

Face aux inconvénients que présentent aussi bien la théorie de l'émission que la théorie de la réception, certains préconisent d'appliquer la théorie de l'ubiquité qui consiste en une application des deux théories précédentes : Elle permet de localiser " *l'infraction indifféremment aux lieux de manifestation de l'action et de survenance du résultat* "[15].
Elle a l'inconvénient majeur de réunir les inconvénients des deux autres théories, mais peut se justifier par les principes du droit pénal.

L'art. 113-2 CP prévoit en effet que " *la loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* ". Si l'on associe cette disposition à celles des art. 113-6 et 113-7 CP qui prévoient l'application de la loi pénale française (sous quelques conditions tout de même) lorsque l'infraction est commise, même à l'étranger, par un Français ou contre un Français, l'on obtient une application quasi-générale de la loi pénale française.
De ce fait, toute infraction commise via Internet serait susceptible d'être appréhendée par la loi pénale française dès lors que l'un d'un de ses éléments se serait manifesté en France, sans exiger de conditions telles une réciprocité d'incrimination ou un degré particulier de gravité de l'infraction. Ainsi, lorsque le site de l'école Polytechnique est piraté depuis l'Israël[16], ou lorsqu'un forum distribué par un serveur français diffuse à travers le monde des images pédophiles, la loi française est applicable.

Après tout, la théorie de l'ubiquité a déjà été appliquée par la jurisprudence, souvent en réponse à une question de compétence juridictionnelle (les questions de l'application de la loi et de la compétence juridictionnelles étant souvent confondues) : Ont été réputés commis en France la contrefaçon d'un ouvrage

[11] Trib. Police Paris 9 juin 1997 Ass° Défense de la langue française, Avenir de la langue française c/ Ass° Georgia Tech Lorraine – " au fil du Net " Gaz. Pal. 10, 12 août 1997 p.25 - Gaz. Pal. 19, 21 oct. 1997 som. P.41
[12] les associations ont fait appel
[13] Notons que depuis le jugement du 9 juin 1997, Georgia Tech Lorraine a modifier son site pour proposer ses informations en anglais, français et allemand et indique que les liens hypertexte qu'il offre pointent vers des sites en langue anglaise.
[14] " Publicité sur Internet : droit et déontologie "N. Varille Gaz. Pal. 21,22 nov. 1997 p.5
[15] *Droit pénal international* Huet & Koering-Joulin coll. Thémis éd. PUF 1994 p.214
[16] le 2 juin 1996 - dans *Internet et la loi* T. Piette-Coudol & A. Bertrand coll. Dalloz Service éd. Dalloz 1996 p.60

français par un ouvrage américain édité et diffusé aux Etats-Unis[17], la reproduction à l'étranger de modèles déposés de carrosserie d'automobiles françaises[18], l'ancien outrage aux bonnes mœurs dont l'auteur avait pris les photos en France et les avait pourtant expédié à l'étranger[19]. La jurisprudence et même la législation en matière de publicité prohibée (art. L. 556 CSP par exemple en matière de publicité pour les médicaments) considèrent que la loi pénale française s'applique dès lors que la publicité est reçue ou perçue en France. Cette théorie est même reconnue en matière de diffamation par la Cour de Justice des Communautés Européennes[20] qui a estimé que le droit applicable était celui désigné par les règles de conflit de lois du droit national de la juridiction saisie.

Nous l'avons écrit, cette conception a l'inconvénient de soumettre l'utilisateur à toutes les législations dans la mesure où la plupart des services sont susceptibles d'être perçus aux quatre coins de la planète. Retenir le critère de la spécificité de la destination du message serait peut-être un moyen de limiter les abus de cette théorie.

Il ressort de cette étude que la solution qui semble préférable est peut-être que les Etats s'entendent pour adopter la théorie de l'émission et permettre l'application de la théorie de la réception lorsque la première ne peut jouer. C'est un peu la solution adoptée par la directive " Télévision sans frontières " qui pose le principe selon lequel les Etats doivent veiller à ce que les organes de télédiffusion respectent les règles de l'Etat émetteur, mais permettent aux Etats qui reçoivent les programmes de les suspendre dans des conditions strictes.

Certains auteurs[21] vont plus loin et préconisent l'adoption non plus de règles internationales concernant l'application de la loi pénale, spécifiques à Internet, mais de dispositions réglementant de façon complète les litiges liés à Internet, soit par une " Lex Cybernautica "[22], soit par une loi supranationale.

II. RELATIVITE DES DIFFICULTES

Les solutions présentées ci-dessus ont l'inconvénient de ne résulter que de l'étude du droit pénal français. Or Internet ne connaît pas de frontières : les principes de règlement des conflits positifs de compétence et l'autorité des jugements étrangers s'avèrent bien dérisoires. Il faut donc sans doute privilégier une solution ayant le même caractère que la difficulté à laquelle elle répond, c'est à dire internationale. Deux solutions sont alors envisageables.

1. 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* "[23]. Celle-ci se présente sous la forme de dix commandements[24] :

1.Tu n'emploieras pas l'ordinateur pour nuire à autrui.
2.Tu ne brouilleras pas le travail informatique d'autrui.
3.Tu ne fouineras pas dans les fichiers des autres.
4.Tu n'emploieras pas l'ordinateur pour voler.
5.Tu n'emploieras pas l'ordinateur pour faire de faux témoignages.
6.Tu n'emploieras, ni ne copieras du logiciel que tu n'as pas payé.
7.Tu n'emploieras pas les ressources informatiques d'autrui sans autorisation.
8.Tu ne t'approprieras pas le travail intellectuel d'autrui.
9.Tu songeras aux conséquences sociales du programme que tu écris.
10.Tu emploieras l'ordinateur de manière à faire preuve de considération et respect.

[17] Crim. 2 fevr. 1997 Bull. Crim. n°41
[18] Crim. 6 juin 1991 Bull. Crim. n°240
[19] Crim. 4 juill 1969 Bull. Crim. n°190
[20] CJCE 7 mars 1995 D.1996. 61 qui permet à la victime d'une diffamation par voie de presse d'agir auprès des juridictions de l'ensemble de Etats contractants de la Convention de Bruxelles du 27 septembre 1968 dans lesquels a été diffusé l'article diffamant
[21] " Cybermonde : Droit et droits des réseaux " M. Vivant JCP 1996 II. 3969
[22] " Libres propos pour une " Lex Cybernautica " " J.C. Galloux dans " Expertises pour l'an 2000 " éd. Des Parques
[23] " 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
[24] en provenance du Computer Ethics Institute – http://www.fau.edu/rinaldi.net

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* "[25].

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[26]. 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[27]. 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*[28]) mais pas le prononcé de sanctions de nature pénale.

2. Un droit international

Seul le droit peut avoir cet aspect contraignant. Or, pour trouver une solution unique et juridique aux comportements contestables qui peuvent s'exprimer par Internet, il faut une réponse internationale. Celle-ci peut se présenter sous deux formes.

La première réponse consiste à définir les infractions de façon unique au niveau international.
Nombre de comportements sont considérer comme répréhensibles par toutes les législations. Les difficultés relative à la détermination de la loi applicable ne portent alors que sur des " détails ", qui ont souvent leur importance : dans ces hypothèses, les législations sont d'accord sur l'idée de l'incrimination mais divergent quant à la définition exacte de l'infraction, de son auteur, aux sanctions encourues, aux particularités procédurales, divergences qui entraînent des situations fortes différentes pour leurs auteurs selon la loi applicable. Il existe d'autres comportements dont le caractère légal ou non n'est pas identique dans tous les pays ;l'exemple le plus médiatique est sans doute le négationnisme, mais on peut citer également les sanctions encourues en cas de violation de dispositions commerciales (TVA, publicité..). Dans les deux cas, une concertation internationale pour dégager des règles communes, voire la compétence d'une juridiction unique,

---

[25] 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 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

[26] 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

[27] 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.* "

[28] " Libres propos pour une " Lex Cybernautica " " J.C. Galloux dans " Expertises pour l'an 2000 " éd. Des Parques

serait l'idéal. Mais cette solution est sans doute chimérique : cette concertation serait trop laborieuse, notamment en ce qui concerne le second type d'infractions, et délaissée par les Etats qui rechignent toujours à abandonner une part de leur souveraineté. Des actions communes sur quelques sujets sont tout de même envisageables à l'instar d'autres matières.

De façon plus réaliste, un accord international portant sur les règles de détermination de la loi applicable dans le cadre des infractions commises via Internet serait envisageable. La difficulté résidera alors dans le fait de ne pas laisser aux délinquants trop de facilités pour échapper à la répression. Notons que la question de la compétence juridictionnelle pourrait y être également abordée[29].

Quelle que soit la solution adoptée, elle devra être internationale pour être efficace. Le droit pénal international semble promis à un bel avenir.

B. LA RESPONSABILITE DES ACTEURS

A la complexité des situations géographiques des acteurs, s'ajoute la diversité de ces derniers. Il faut régler le sort des utilisateurs et des auteurs mais également d'autres intermédiaires que sont les éditeurs de contenus, les serveurs d'hébergement, qui peuvent être les premiers à héberger un serveur ou se contenter de reproduire un serveur (serveurs miroirs), les fournisseurs d'accès, les transporteurs. De plus, ces fonctions peuvent se cumuler.

Par exemple, un fournisseur d'accès peut être le serveur d'hébergement du site que l'on veut consulter, ou l'a reproduit pour la consultation (site miroir). Ce serveur d'hébergement peut également être l'éditeur de contenu de la même manière qu'il peut être le serveur d'hébergement d'un site dont l'auteur est, ou n'est pas, l'éditeur de contenu.

Ce qui est relativement clair, c'est que **l'auteur** doit être responsable de ce qu'il émet.

Par contre, la question de la responsabilité se pose pour les autres intervenants.

I. L'ETAT ACTUEL DE LA QUESTION

Le législateur (1.), ainsi que les juridictions (2.), ont tenté de clarifier les conditions de responsabilité pénale des acteurs d'Internet.

1. L'amendement Fillon

Pour les fournisseurs d'accès

En 1996, le Ministère des Postes et des Télécommunications a voulu clarifier la responsabilité des fournisseurs d'accès à Internet, dans un sens qui leur était favorable[30].

Il est vrai que ces fournisseurs d'accès, lorsqu'ils ne sont ni éditeur de contenu, ni fournisseur d'hébergement, ne font que donner accès au réseau.

Un projet de loi fut voté par le Parlement le 18 juin 1996.

Ce texte rajoutait à la loi du 30 septembre 1986 relative à la liberté de communication trois articles.

- Art. 43-1 qui imposait au fournisseur d'accès à un service de communication audiovisuelle de proposer à leurs clients un moyen technique leur permettant de restreindre l'accès à certains services ou de les sélectionner.
- Art. 43-2 qui créait un Comité de la Télématique (une extension du Conseil de la Télématique) dôté d'importants pouvoirs dont celui de communiquer des avis aux services de communication qui ne respecteraient pas les règles déontologiques dégagées par lui, voire de publier ces avis au Journal Officiel.
- Art. 43-3 énonçait le principe d'irresponsabilité pénale des fournisseurs d'accès dès lors que trois conditions étaient respectées :
  - ♦ Le fournisseur d'accès doit avoir respecté les dispositions de l'art. 43-1 (l'art. 43-3 prévoyait donc les sanctions de l'art. 43-1)

[29] On pourrait alors opter soit pour la compétence des juridictions de l'Etat dont la loi est applicable, soit pour la compétence de toute juridiction de l'Etat lié à l'infraction d'une manière prédéfinie, soit pour la compétence d'une juridiction internationale.

[30] F. Fillon " *On ne saurait tenir un transporteur d'informations responsable des informations qu'il transporte* " RMC 10 mai 1996 (dans " Internet pour les juristes " N. Totello & P. Lointier éd. Dalloz)

- Le fournisseur d'accès ne doit pas avoir laisser accéder à un site qui a fait l'objet d'un avis défavorable du Comité, publié au Journal Officiel
- Le fournisseur d'accès ne doit pas avoir, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission.

Quelques remarques sur ce projet de loi sont importantes. Ce texte, au lieu de protéger les fournisseurs d'accès, leur était plutôt défavorable car en multipliant les conditions a remplir pour être pénalement irresponsable, multiplier également les hypothèses de responsabilité. De plus, le texte réglait également indirectement le sort des fournisseurs d'accès qui donnait accès à un serveur qu'il hébergeait dans l'art. 43-3.

Le Conseil Constitutionnel, dans une décision du 23 juillet 1996[31], déclara inconstitutionnel l'art. 43-2 en ce qu'il ne respectait pas l'art. 34 de la Constitution car il n'imposait pas de limites suffisamment précises aux pouvoirs du Comité alors que des sanction pénales pouvaient en découler. L'art. 43-3 fut également déclaré inconstitutionnel par voie de conséquence.

Seul l'art. 43-1 fut intégré à la loi du 30 septembre 1986 par la loi du 26 juillet 1996. Et cet article emporte des conséquences quant à la situation des fournisseurs d'accès.

- L'art. 43-1 n'est plus sanctionné pénalement (puisque la sanction était prévue par l'art. 43-3)
- L'art 43-1 qui est applicable tend à s'appliquer aux fournisseurs d'accès à Internet. Or le texte vise les fournisseurs d'accès à des services de *communication audiovisuelle* et se situe dans une loi qui régie la liberté de communication en matière audiovisuelle.
  De ce fait, Internet est reconnue comme proposant au moins en partie des services de communication audiovisuelle. Reste à savoir quels sont ces services (on peut d'ores et déjà exclure le courrier électronique).

2. L'attitude des tribunaux

Jusqu'à présent, les juridictions ne se sont prononcées quasiment qu'en matière de référé. Leur attitude face aux acteurs est donc essentiellement valable en matière civile, mais elle permet de dégager une tendance. Nous pouvons dégager deux attitudes, qui se sont succédées.

a) Eluder la question en s'en déchargeant

pour les fournisseurs d'accès et transporteurs

La première décision importante en la matière était l'ordonnance de référé rendue par le TGI de Paris le 12 juin 1996[32]. L'Union des étudiants juifs de France avait décidé d'assigner huit fournisseurs d'accès à Internet et un transporteur (Renater) en référé pour leur interdire de permettre l'accès à tout service diffusant les messages incriminés par l'art. 24bis de la loi du 29 juillet 1881 (apologie des crimes contre l'Humanité) et ce qu'ils soient également fournisseur d'hébergement au profit de ses services ou non.

Il faut savoir que un fournisseur d'accès ne peut bloquer l'accès à un site dont il n'est pas l'hébergeur qu'en bloquant l'accès au serveur d'hébergement de ce site. Donc, si un fournisseur d'accès le fait, il bloque également l'accès à tous les autres sites hébergés par ce service.

Le TGI de Paris refusa de trancher en considérant qu' " *il est défendu aux juges de prononcer par voie de disposition générale et réglementaire sur les causes qui leur sont soumises ; que par ailleurs, la liberté d'expression constitue une valeur fondamentale, dont les juridictions de l'ordre judiciaire sont gardiennes, et qui n'est susceptibles de trouver de limites, que dans des hypothèses particulières, selon des modalités strictement déterminées.* ".

De plus, le tribunal pris acte des engagements que prenaient les défendeurs et qui sont tous différents les uns des autres : certains (Calvacom, Internet way, Imaginet, Francenet) reconnaissent que leur responsabilité pourrait être engagée en raison des messages émis sur les sites web et forums dont ils sont " *les concepteurs, les animateurs et/ou qu'ils hébergent volontairement pour les diffuser, soit pour leur propre compte, soit pour le compte de tiers, abonnés ou annonceurs, auxquels ils sont contractuellement liés* ", d'autres (Axone,Olénae) excluent toute responsabilité de leur part et s'engagent uniquement à prendre des mesures contre les sites qu'ils hébergent ou éditent, enfin Renater élude la question.

[31] Cconst. N° 96-378 DC 23 juill 1996 – JO 27 juill 1996
[32] http://www.celog.fr/expertises

Pour les fournisseurs d'hébergement

Dans son ordonnance de référé du 5 mai 1997, le TGI de Paris[33] élude également la question. Le demandeur agissait contre l'auteur d'une page web contrefaisant des poèmes de Raymond Queneau, mais également contre l'Université et l'association universitaire dont le serveur hébergeait ces pages. Le tribunal se déclara incompétent sur le fond.

b) Eluder la question en ne poursuivant que l'auteur

C'est la voie qu'a suivie le TGI de Paris en matière de diffamation dans une ordonnance de référé du 16 avril 1996[34]. Un chef d'entreprise avait reproduit sur Internet des propos diffamatoires à l'encontre de deux banques. Le tribunal n'a retenu que la responsabilité de l'auteur, en lui faisant remarquer qu'il ne saurait faire valoir " *qu'aucun contrôle de l'accès et de la diffusion des informations sur le réseau ne peut être exercé, dès lors que toute personne ayant pris la responsabilité de faire diffuser publiquement, par quelque mode de communication que ce soit, des propos mettant en cause la réputation d'un tiers doit être au moins, en mesure, lorsque cette divulgation est constitutive d'un trouble manifestement illicite, de justifier des efforts et démarches accomplis pour faire cesser l'atteinte aux droits d'autrui*. ".

De la même façon, le tribunal correctionnel de Privas, en septembre 1997[35] n'a poursuivi pour mise en mémoire informatique, sans consentement de l'intéressée, de données sensibles qui directement ou indirectement font apparaître ses mœurs, que le jeune homme qui avait installé les photos et le texte litigieux.

La Cour Suprême des Etats-Unis est allée plus loin en tranchant la question en faveur des serveurs d'hébergement[36]. Elle considère que le fournisseur d'accès à Internet n'est pas responsable des informations auxquelles elle donne accès, y compris celles qu'elle héberge sur son serveur, en raison de la particularité du réseau, où tout contrôle des informations est impossible du fait de leur circulation très rapide. Sa connaissance de l'existence de messages préjudiciables ne porte pas atteinte à son irresponsabilité, la Cour considérant que si le professionnel intervient pour supprimer ces messages, il ne fait que se conduire en " bon samaritain ".

c) Exceptions

En France, quelques juridictions ont décidé de poursuivre des intermédiaires, mais les poursuites ne sont pas suffisamment avancées pour en tirer des conséquences sur la responsabilité de ces acteurs.
Ainsi, les gérants de serveurs d'hébergement également fournisseurs d'accès (World Net et FranceNet) ont été mis le 7 mai 1996 en examen par le premier juge d'instruction parisien Christine Berkani[37] du chef de diffusion et de transmission d'images pornographiques de mineurs. Le gérant de FranceNet conteste d'ailleurs que sa responsabilité puisse être engagée pour des messages auxquels il ne fait que donner accès.[38]. La question n'a pas encore été débattue. Nous en sommes au même stade dans l'affaire de pédophilie jugée par le Tribunal du Mans[39] puisque la question se pose de la responsabilité du fournisseur d'accès. Celui-ci pourrait être poursuivi pour transport ou diffusion d'un message à caractère pornographique susceptible d'être perçu par un mineur ou pour complicité de recel

Une ordonnance de référé du 9 juin 1998[40] du TGI de Paris semble annoncer une responsabilité des serveurs d'hébergement. Elle précise 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 ". Il est ajouté que " pour pouvoir s'exonérer de sa responsabilité, il devra 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 ".

---

[33] TGI Paris 5 mai 1997 – JCP 1997 éd. G. II. 22906
[34] TGI Paris ord. Réf. 16 avril 1996 BNP et autres c/ Rocher - D. 1997 som. Com. P72
[35] http://www.celog.fr/expertises
[36] Cour Suprême 22 juin 1998 Zeran v. América Online (Expertises sept. 1998 – http://www.legalis.net) : dans le cadre d'un procès intenté par un photographe contre AOL qui publiait sur son serveur des messages de tiers qui lui causaient des désagréments : ces messages prétendaient que le photographe assurait la vente de T-shirt portant des slogans vulgaires et agressifs à propos de l'attentat d'Oklahoma.
[37] " Internet pour les juristes " N. Tortello & P. Lointier éd. Dalloz
[38] voir le communiqué de FranceNet du 13 mai 1996 à ce sujet " Comment devenir pédophile en 24h " http://www.francenet.fr/comment/comment.html
[39] TCorr. Le Mans – 16 fév 1998 – http://www.legalis.net – Expertises mars 1998 (http://www.celog.fr)
[40] informations de juillet 98 http://www.legalis.net)

II. LES DIFFERENTES SOLUTIONS

Soit on tente de rattacher Internet à une qualification juridique préexistante, soit on reconnaît son autonomie.

1. L'assimilation d'Internet à une qualification préexistante

Qualifier Internet selon les catégories juridiques qui existent signifie le soumettre au régime de cette catégorie.

Internet relève sans aucun doute de la télécommunication, cette dernière se définissant selon l'art. 2 de la loi du 30 septembre 1986 comme " *toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par fil, optique, radio-électricité ou autres systèmes électromagnétiques* ".
Il faut rappeler que la loi du 10 avril 1996 sur les expérimentations en matière d'autoroutes de l'information écarte ces qualifications pour certains services.

Or, on distingue en matière de télécommunication la correspondance privée de la communication audiovisuelle.
La **communication audiovisuelle** se définit comme " *toute mise à disposition du public ou de catégories de public, par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* " (art. 2 L. 30 sept. 1986).
La **correspondance privée**, par contre, n'a pas de définition légale. Seule la circulaire du 17 février 1988 en donne une définition : il faut qu'il y ait un " *message exclusivement destiné à une (ou plusieurs) personnes, physique ou morale, déterminée et individualisé* ". Un arrêt de la Cour d'Appel de Metz[41] avait précisé qu'il fallait non seulement que l'appel soit personnel, libre et privé, mais que l'ensemble de l'échange téléphonique devait l'être aussi et qu'il ne devait présenter aucune volonté positive et formelle de porter un acte de communication au public.
Internet devrait donc relever de l'une ou de l'autre des qualifications. Mais deux difficultés se posent.

a) La difficulté de qualifier Internet

Internet revêt différents aspects. Il est certain que le courrier électronique s'apparente à une correspondance privée, tandis qu'un site web à tous les aspects d'une communication individuelle.

Mais pour certains services, la qualification est très difficile.
La **liste de diffusion** emprunte la technique du courrier électronique, mais est destinée à un nombre de personnes qui peut être très important.
Les **forums de discussions** sont sans doute également d'une nature hybride. Certains ont des conditions d'admission très libres et des thèmes de discussion non contrôlés. D'autres sont réservés à des personnes ayant un intérêt en commun ou ayant adhéré et sont modérés (un *modérateur* organise la discussion).
Intranet pose aussi une difficulté de qualification. La circulaire de 1988 considérait comme une correspondance privée les services à caractère professionnel qui, au sein d'un organisme, d'une administration, d'une organisation professionnelle, d'une entreprise, sont exclusivement destinés à ses employés, représentants ou adhérents. De plus, la jurisprudence considère que le personnel d'une entreprise constitue un groupement de personnes liées par une communauté d'intérêt et n'est donc un public au sens des dispositions relatives à la presse. Intranet relèverait donc de la correspondance privée.

Or le législateur n'a pas fait de distinction, notamment dans la loi du 26 juillet 1996 qui semble faire d'Internet un service de communication audiovisuelle. De plus, les juridictions ne semblent pas non plus apprécier ces différences de natures des services : le tribunal correctionnel de Privas a considéré en septembre 1997 *" qu'Internet est un service de communication audiovisuelle "* sans distinguer en fonction des services.

b) Les difficultés créées par les conséquences de la qualification

[41] Cap Metz 18 juill. 1980 " Internet et la loi " T. piette-Coudol & A. Bertrand éd. Dalloz p. 79

Qualifier certains services d'Internet de correspondances privées signifient les soumettre au régime de cette correspondance.
Mais si quelques-unes unes des applications d'Internet sont des services de communication audiovisuelle, cela signifie que ces services doivent être soumis à l'ensemble des dispositions relatives à la communication audiovisuelle de la loi du 29 juillet 1982, comme entre autre :

- L'obligation de déclaration préalable au Procureur de la République et au CSA(art. 86)
- L'obligation de déclaration à la CNIL dans certaines hypothèses
- L'obligation d'avoir un directeur de publication (art. 93-2)
- L'application des dispositions du chapitre IV de la loi du 29 juillet 1881
- Le régime de responsabilité en cascade (art. 93-3) " *lorsque le message incriminé fait l'objet d'une fixation préalable à sa communication au public* ", pour les infractions précitées et celles pour lesquelles le Code Pénal prévoit une responsabilité de ce type.

  La fixation préalable est d'ailleurs une difficulté supplémentaire. En effet, ce n'est parce que certains fournisseurs d'accès reproduisent le contenu de serveurs (afin de les fournir plus rapidement à leurs abonnés) qu'ils peuvent en contrôler le contenu.

2. L'autonomie d'Internet

Il semble que ce soit la conception qui doive s'imposer.

Comme l'a fait remarquer le rapport Falque-Pierrotin[42], " *Il faut reconnaître..le caractère spécifique et profondément novateur de l'Internet qui interdit toute transposition automatique de schémas préétablis ; l'Internet n'appartient ni au monde de la diffusion, ni à celui de la télématique ; il bouscule les définitions classiques du droit de la communication fondées sur la distinction entre correspondance privée et communication audiovisuelle ; c'est en réalité un monde d'utilisateurs, la plupart identifiés, qui passent par différents réseaux interconnectés, grâce à un protocole de communication non propriétaire, pour aller chercher l'information et le service dont ils ont besoin et les rapporter sur leurs ordinateurs.* ".

Nous l'avons dit, il existe deux régimes de responsabilité envisageables à l'égard des fournisseurs d'accès, serveurs d'hébergement et transporteurs.
Ces deux solutions ont d'ailleurs été étudiées par le rapport Falque-Pierrotin.

a) Un régime de responsabilité en cascade

Ce régime s'inspirerait de celui qui existe en matière de presse et d'audiovisuel. Le rapport Falque-Perrotin propose alors d'établir la " cascade de responsabilité " comme suit :

- éditeur de contenu
- auteur
- fournisseur d'hébergement

Le fournisseur d'accès et le transporteur n'engagerait par contre sa responsabilité que s'il commet l'infraction personnellement ou en est complice.

Si ce régime de responsabilité présente des avantages au profit des victimes, de la rapidité de la justice, certains inconvénients sont indéniables. Les fournisseurs d'hébergement ont le plus souvent l'impossibilité matérielle de vérifier le contenu des informations qu'ils hébergent : d'une part, ces informations sont trop nombreuses et sont modifiées trop souvent pour qu'un contrôle efficace soit effectué. De plus, nombre de ces informations doivent être décompressées pour être contrôlées. A terme, cela risque de décourager l'installation en France de serveurs d'hébergement, ce qui aurait des conséquences dommageables sur la place de la France dans la société des autoroutes de l'information.

b) Un régime de responsabilité de droit commun

Ce régime est beaucoup plus souple puisqu'il exigerait de rapporter la preuve de l'intention coupable des personnes poursuivies. C'est une solution d'ailleurs conforme au droit commun de la responsabilité pénale, exprimé par l'art. 121-1 CP " *Nul n'est responsable pénalement que de son propre fait* ". De plus, leur responsabilité pourrait être engagée en tant que complice lorsque les fournisseurs et opérateurs auront eu la

[42] Rapport Falque-Pierrotin précité. p. 8

conscience et l'intention de s'associer à la commission d'un crime ou d'un délit (art.121-7 CP). Les difficultés soulevées à l'encontre de la responsabilité présumée des fournisseurs d'hébergement seraient ainsi évacuées. De plus, cela permettra une meilleure adaptation aux nouvelles situations qui ne manqueront pas d'être créées.

Toute la difficulté résidera dans le fait d'établir dans quelles hypothèses le fournisseur d'hébergement sera responsable du contenu qu'il héberge (de même pour le fournisseur d'accès et le transporteur).

Trois conditions cumulatives semblent se dégager pour que leur responsabilité pénale soit engagée. Tout d'abord, il faudrait que le message litigieux soit fixer sur le serveur de l'acteur poursuivi. Cette condition est liée aux deux suivantes : si le message est fixé, cet acteur a connaissance de l'information et peut y mettre fin. De ces conditions de responsabilité, il ressort que les fournisseurs d'accès(à moins de reproduire sur son propre serveur les documents les plus visités, dont le message délictueux) et les opérateurs seront rarement responsables, à l'inverse du serveur d'hébergement.

Peut-être tiendra-t-on compte également des engagements que peut prendre le fournisseur à l'égard de ses abonnés comme des juridictions américaines l'ont fait : en matière de diffamation, un fournisseur d'hébergement fut condamné car il se présentait comme exerçant un contrôle éditorial strict[43] tandis qu'un autre échappa à toute condamnation car il était connu pour n'exercer qu'un très faible contrôle sur ses babillards[44]

§2. LES DIFFICULTES TECHNIQUES

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

A. LA CRYPTOLOGIE[45]

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* "[46].

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[47]…D'où la nécessité de le réglementer, selon la France, pour en limiter l'utilisation. Mais dès lors qu'on l'autorise, se pose la difficulté de pouvoir décoder quand on en aura besoin certains messages.

I. LE FONCTIONNEMENT

[43] Stratton Oakmont Inc.v. Prodigy Services Co. 1995
[44] Cubly v. CompuServe Inc. 1991
[45] *La sécurité informatique* C. Jan & G. Sabatier éd. Eyrolles 1989 – " Cryptographie : les enjeux et l'état de la législation française " V. Sédallian http://www.argia.fr/lij – " Cryptologie : le nouveau régime juridique " P.Lagarde Gaz. Pal. 1996 n° 299-300 p.49 – " L'Europe veut libéraliser l'usage d cryptage sur la Toile " Le Monde 8 nov. 1997 p.23 – l'état de la législation sur la cryptologie http://www.aui.fr
[46] " La protection des données sur les autoroutes de l'information " P. Nicoleau D. 1996 chron. P.111
[47] *Cyber mafias* S. Le Doran & P. Rosé 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.

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.

II. LA REGLEMENTATION

La France ne connaît que depuis peu de temps une attitude favorable à la cryptologie, attitude qui demeure restrictive. Auparavant[48], les moyens cryptologiques étaient considérés comme des armes de guerre dont l'utilisation était soumise à autorisation ou déclaration préalable.

La loi du 26 juillet 1996[49] a amorcé une libéralisation de la cryptologie. Elle distingue plusieurs types de régimes en fonction de la provenance des logiciels et de leur complexité.

- La fourniture, l'importation, l'exportation hors Communauté européenne doivent faire l'objet d'une autorisation préalable accordée par le Service central de la sécurité des systèmes d'information (SCSSI). Mais si le logiciel a pour fonction d'assurer la confidentialité, toutes ces activités sont interdites (ainsi, le logiciel PGP[50] ne peut être utilisé en France).
- Dans les autres hypothèses, il n'y a plus nécessité ni d'autorisation, ni de déclaration préalable.
  - Lorsque les moyens n'assurent pas la confidentialité, ils sont d'utilisation libre. Ces moyens n'assurant pas la confidentialité sont ceux utilisant des algorithmes reposant sur des clés de moins de 40 bits, c'est-à-dire facilement " cassables ".
  - Lorsque les moyens assure la confidentialité, les utilisateurs doivent recourir aux services de tiers de confiance[51], qui sont des organismes agréés par le Premier Ministre.

Toute la difficulté de la législation relative à la cryptologie était de concilier deux impératifs : assurer la confidentialité des communications pour permettre le développement de ce mode de communication, et éviter d'en faire un outil de communication inviolable au profit des délinquants, d'autant plus que le cryptage complique le travail des enquêteurs en ce qu'il allonge les enquêtes et augmente leurs coûts. D'où cette législation qui semble assurer aux autorités les moyens de prendre connaissance des informations échangées de trois façons.

1° Interdire les logiciels de cryptage non développés en France

Dont on pourrait penser, éventuellement, qu'ils sont dangereux car les autorités françaises ne pourront pas se procurer les clés…

2° Autoriser des logiciels, mais de puissance limitée

Les décrets autorise des logiciels de cryptage utilisant des clés à 40 bits (voire prochainement à 56). Or, l'expérience a montré que de telles clés sont très faciles à casser : en 1995, un informaticien, Damien Doligez réussit à casser un tel code en quelques heures en utilisant 112 ordinateurs de l'INRIA.

3° Confier les clés des autres logiciels à des tiers de confiance

[48] Dt 12 mars 1973 – Dt 18 fév 1986

[49] loi n°96-659 du 26 juillet 1996 de réglementation des télécommunications - J.O. 27 juillet 1996
Dt. n° 98-101 du 24 février 1998 J.O. 25 février 1998 p.2911 – Arrêté du 13 mars 1998 J.O. 15 mars 1998 p.3886 – Dt n° 98-206 du 23 mars 1998 J.O. 25 mars 1998 p.4448

[50] PGP : *Pretty Good Privacy*, cet algorithme de cryptographie repose sur une clé de 128 caractères, ce qui le rend quasiment incassable puisqu'il faudrait, en utilisant un milliard de microprocesseurs capables de tester un million de clés par seconde, dix mille milliards d'années pour essayer toutes les clés dont PGP permet l'utilisation. (*Guerres dans le cyberespace* J.Guisnel éd. La Découverte p. 71 – *Cyber mafias* S. Le Doran & P. Rosé éd. Denoël p.123)

[51] Dt n°98-102 du 24 février 1998 J.O. 25 février 1998 p.2915 – trois arrêtés du 13 mars 1998 J.O. 15 mars 1998 p.3888 & s.

La loi prévoit que ces tiers de confiance à qui seront confié la gestion des clés devront communiquer aux autorités judiciaires les clés dans les conditions prévues par la loi du 10 juillet 1991 relative au secret des correspondances par voie de télécommunications [52](nous y reviendrons ultérieurement). La non-soumission à cette obligation est d'ailleurs sanctionnée de 6 mois d'emprisonnement et de 200 000 F d'amende.

En prenant ces dispositions relatives à la cryptologie, la France a démontré sa volonté d'agir contre certains néfastes des réseaux. Mais la réglementation qu'elle a adopté présente de nombreux inconvénients.

III. LES DEFAUTS DE CETTE REGLEMENTATION

Tout d'abord, la France est le seul pays occidental a avoir réglementé l'usage de ces logiciels et a avoir une telle attitude de méfiance à l'égard de la cryptologie. En effet, les Etat-Unis[53], le Royaume-Uni, le Canada, l'Allemagne et l'Italie permettent une utilisation libre de ces logiciels. Cette position constitue un double inconvénient pour la France : le principe même de la réglementation constitue un obstacle au commerce électronique. De plus, le problème de la cryptologie doit être étudié de façon internationale : si la France conserve une attitude divergente, nous serons toujours confrontés à des difficultés d'application de la réglementation face à des situations contenant des éléments d'extranéité et les entreprises françaises travaillant dans ce secteur seront défavorisées. C'est donc parce que " *l'Union européenne ne peut en aucun cas se permettre d'avoir un paysage réglementaire fragmenté dans un domaine* (le commerce électronique) *aussi vital pour l'économie et la société* " que la Commission européenne a rendu le 8 octobre 1997 une communication[54] tendant à unifier les réglementations des Etats européens[55]. A titre transitoire (jusqu'au 1er juillet 1998), le règlement Double Usage[56] prévoyait que l'exportation dans et hors Union de la catégorie des " biens sensibles ", dont font partie les produits de chiffrement, devait faire l'objet d'une autorisation. Désormais, la Commission souhaite favoriser la libéralisation de leur circulation car elle considère que " *toute réglementation limitant l'usage de produits et de services de chiffrement dans le marché intérieur constitue un obstacle à la libre circulation des informations personnelles et à la fourniture des biens et des services qui y sont liés* ". Elle prévoit d'ailleurs la mise en place d'un cadre commun à travers l'Union d'ici l'an 2 000, tandis que le Conseil prépare une recommandation sur le sujet.

De plus, les utilisateurs de logiciels de cryptage sont très méfiants à l'égard des tiers de confiance (à tel point qu'ils les appellent " tiers de méfiance ") dont ils craignent une collaboration trop étroite avec les autorités judiciaires et administratives.
La question se pose d'ailleurs actuellement de savoir quelles entreprises se proposeront pour assurer ses fonctions. En effet, on fait déjà valoir[57] que, compte tenu du coût des infrastructures à mettre en place pour obtenir l'agrément, les prestations coûteront cher aux utilisateurs, ce qui fera de l'activité une activité peu rentable, voire risquée.

Enfin, on peut douter de l'effet persuasif des incriminations crées pour assurer le respect de cette réglementation :

- Le fait d'importer un logiciel de cryptage d'un pays extérieur à la Communauté est puni de 6 mois d'emprisonnement et de 200 000 F d'amende.

Comment peut-on matériellement contrôler que tous les ordinateurs ne contiennent pas ce type de logiciel alors que des sites les diffusent ?

---

[52] arrêté du 13 mars 1998 J.O. 15 mars 1998 p.3891
[53] Il faut souligner que les Etats-Unis connaissent une évolution constante de l'attitude face à la cryptologie : d'abord de circulation libre au sein du pays, mais interdits d'exportation en tant que munitions, les logiciels de cryptage ont bénéficié de décisions prononçant l'inconstitutionnalité de cette restriction à leur exportation, sur le fondement d'une atteinte à la liberté d'expression (Cour du District Nord de Californie *Bernstein v. US Dpt of State* 16 déc. 1996 – Gaz. Pal. 6,8 avril 1997), ainsi que de décisions en sens contraire (*Trib. Fédéral de l'Ohio Junger v. US dpt of State* août 98 – Le Monde supplméent multimédia 16, 17 août 1998). En 1993, l'administration avait tenté d'introduire un contrôle du cryptage par l'installation dans tous les ordinateurs d'une puce pirate (*clipper chip*) permettant aux autorités de décoder les messages, projet abandonné en1994 après les protestations des internautes. Mais, sur la pression du FBI, et d'industriels de l'informatique, le gouvernement et le Congrès envisagent à nouveau un contrôle des clés par le système du *key recovery* (*Guerres dans le Cyberespace* J. Guisnel éd. La Découverte p.92 - Le Monde 28 mars 1998 p.23)
[54] Communication de la Commission du 8 oct 1997 " Assurer la sécurité et la confiance dans la communication électronique – Vers un cadre européen pour les signatures numériques et le chiffrement " COM(97) 503 final
[55] sur l'invitation du Parlement européen : Résolution du parlement A4-244/96 du 19 sept 1996 JO 320 du 28 oct 1996
[56] Règlement du Conseil (CE) 3381/94 du 19 déc 1994 JO L367/1 du 31 déc 1994
[57] " La France redéfinit sa réglementation en matière de cryptologie " Le Monde 28 mars 1998 p.23

- Le fait d'importer ou d'exporter ce type de logiciel est sanctionné de 3 ans d'emprisonnement et de 500 000 F d'amende lorsque cela a pour but de faciliter la préparation ou la commission d'un crime ou d'un délit.

Nous pouvons faire sur ce point la même remarque que précédemment.
De plus, si la loi tend à viser les délinquants, peut-on croire sérieusement qu'une telle sanction ferait peur à des terroristes ou des trafiquants dont les activités font encourir des peines criminelles ?

B. LA PREUVE

La preuve de l'infraction sera notamment rapportée grâce aux diligences de services spécialisés de police judiciaire. Ces " cyberflics "[58], dont l'activité a été créée pour la plupart en 1994, appartiennent à la police nationale ou à la gendarmerie. Il s'agit du Service d'Enquêtes sur les Fraudes aux Technologies de l'Information (SEFTI)[59], de la Brigade de Recherche et de Répression de la Criminalité Informatique (BRRCI)[60] du Centre Technique de la Gendarmerie Nationale[61] et d'une " cellule Internet " de la police nationale[62].

Il s'agit pour ses services de constater et rapporter la preuve de faits délictueux (I.) ainsi que de découvrir l'identité de leur auteur (II.).

I. LA PREUVE DES FAITS DELICTUEUX

1. Les écoutes

Nous avons étudié que la législation relative à la cryptologie permettait aux autorités judiciaires de se faire communiquer par les tiers de confiance ou de leur faire appliquer les clés, afin de prendre connaissance des messages codés. La loi prévoit que cela doit se faire selon les modalités de l'art. 100 CPP. Ce dernier énonce que " *en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondance émise par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et sous son contrôle. La décision d'interception est écrite.* ".

Si la question des écoutes est réglée par une disposition législative lorsque la communication est codée et que la clé de chiffrement est remise à un tiers de confiance, elle ne l'est pas dans les autres hypothèses.

Afin de disposer des communications comme moyen de preuve, encore faut-il que les autorités judiciaires aient les moyens suffisants, en matériels et en personnels qualifiés, d'intercepter les communications circulant via Internet. En pratique, il leur faut également les moyens de décoder des messages cryptés car nous avons vu que seules des dispositions pénales faisaient obstacles à l'utilisation de logiciels de cryptage efficaces. Or les délinquants, notamment la criminalité organisée, ont des moyens plus importants qui leur permettent d'utiliser de tels logiciels. De plus, il est certain que ces derniers ne respecteront pas les interdictions d'utiliser des logiciels non –européens ou des logiciels puissants sans en confier les clés aux tiers de confiance.

De plus, il faudra déterminer si ces interceptions peuvent se faire sans aucune autorisation ou si elles sont soumises à des dispositions existantes. Il semble qu'il faille reconnaître l'application de l'art. 100 CPP dans cette hypothèse. La condition en sera tout de même comme le prescrit cet article, que la communication interceptée ait un caractère privé. Nous avons déjà fait remarquer que la distinction communication privée/communication publique n'était pas toujours évidente. Il semble toutefois que le courrier électronique bénéficiera de cette protection, à la différence des sites du World Wide Web. En matière de pages web, peut-être que certains justiciables reprendront à leur compte l'argument selon lequel ces pages constitueraient un " domicile virtuel " pour imposer aux autorités judiciaires de respecter les dispositions du Code de Procédure Pénale (art. 57, 76, 96) relatives aux modalités des perquisitions dans un domicile. Cet argument avait été

[58] expression créé par Kevin Manson, instructeur *au Federal Law Enforcement Training Center* au début des années 90 aux Etats-Unis
[59] le SEFTI dépend de la Sous Direction des Affaires Economiques et Financières de la Direction de la Police Judiciaire de la Préfecture de Police de Paris
[60] la BRRCI dépend de la Police Judiciaire nationale
[61] le Centre Technique dépend de la sous-direction des télécommunications et de l'informatique
[62] créée en septembre 1997, cette cellule réunit une douzaine de policiers spécialisés détachés par différents services (" La police française lutte avec difficulté contre la cybercriminalité " Le Monde 22 sept. 1998

invoqué en matière de contrefaçon pour contester le constat par un agent de l'APP de la reproduction d'œuvres musicales protégées sur un site web[63]. Le tribunal n'avait pas examiné la question, la renvoyant à un débat sur le fond après avoir qualifié cette théorie d'originale. Il semble évident que la " lecture " de pages web ne peut pas être soumise au régime des perquisitions de domicile, ni à celui des écoutes téléphoniques, puisque tout à chacun peut les consulter.

Notons que cette question des écoutes pourrait connaître une difficulté si la Chambre Criminelle confirmait la position de la Cour d'Appel d'Aix-en-Provence dans son arrêt du 12 décembre 1996[64]. A propos de policiers qui avaient lu les messages reçus sur un messager de poche (tam-tam) sans respecter les dispositions de l'art. 100 CPP, elle estime que cet acte n'est pas nul car " *bien que le récepteur fonctionne comme un enregistreur de messages acheminés par le réseau des télécommunications, les fonctionnaires de police n'ont en effet procédé ni à un branchement ni à une dérivation pour intercepter les messages enregistrés et contenus sur la bande magnétique de l'appareil de sorte qu'ils ont lus et retranscrits en appuyant seulement une touche comme ils auraient pu saisir une lettre, un télégramme ou un télex* ". Cet arrêt retient en fait deux critères pour qualifier l'absence d'interception :

- l'absence de branchement et de dérivation
- le fait seulement d'appuyer sur la touche de lecture

Si le branchement et la dérivation devait être retenu comme critère de l'interception soumise aux dispositions de l'art.100 CPP, on pourrait se demander si toutes les interceptions de messages circulant sur Internet sont soumises à cet article. En effet, y-aura-t-il vraiment branchement ou dérivation dans le fait d'introduire un programme dans un ordinateur afin que celui-ci rapatrie toutes les données qui transitent par un autre ordinateur ? Il faudrait pour ce faire adopter une conception large de la dérivation et ne pas la limiter à une dérivation matérielle.

Il serait donc bon d'étendre les dispositions de l'art. 100 CPP aux messages transitant par Internet si on décidait qu'ils constituent une catégorie particulière de télécommunication car il faut encadrer toute écoute des autorités publiques de garanties. De même la demande de renseignement aux fournisseurs d'accès ou d'hébergement sur leurs abonnés doit être encadrée[65].

2. La provocation

Les enquêteurs sont amenés pour mettre à jour certaines infractions à commettre des infractions. Ainsi, les policiers qui démantèlent un réseau de pédophiles s'approvisionnant en photos sur le Net doivent " infilter " le réseau et proposer eux-mêmes des photos. Leur acte n'est pas justifié par une permission de la loi car aucune disposition légale, ni réglementaire n'autorise, de façon générale, les enquêteurs à commettre des infractions pour permettre la manifestation de la vérité. Seule la loi du 19 décembre 1991 a crée un tel fait justificatif, au profit des douaniers et officiers de police judiciaires en matière d'enquête relative aux trafics de stupéfiants.

Face aux nouvelles formes que la " grande délinquance " adopte, à son utilisation de plus en plus importante des réseaux de communications, peut-être que la création d'un fait justificatif au profit des enquêteurs serait souhaitable. Cela aurait l'avantage de ne pas se laisser devancer par la criminalité organisée : si celle-ci utilise de plus en plus fréquemment les réseaux comme instrument de commission des infractions, il sera de plus en plus difficile de rapporter la preuve de leurs activités (il n'y aura plus de témoins du vol d'une banque..) et le moyen le plus efficace de rapporter la preuve de l'infraction deviendra de plus en plus d'infiltrer l'organisation. L'inconvénient de ce type de faits justificatifs est de permettre une protection aux enquêteurs qui agiraient pour leur propre compte. C'est pourquoi ce fait justificatif ne serait envisageable que si l'enquêteur a agi dans le cadre d'une procédure stricte, à l'image de celle prévue par la loi du 19 décembre 1991, c'est-à-dire, sur ordonnance du président du TGI, après que ce dernier ait vérifié que ces actes sont nécessaires à la manifestation de la vérité.

3. Le caractère international des infractions

Même si la preuve est assez facile à déceler, il faudra parfois accomplir certains actes à l'étranger. Cela signifie donc passer par une commission rogatoire internationale, ce qui fait perdre beaucoup de temps (les

[63] TGI Paris Ord Réf. 14 août 1996 – Art Music France c/ Ecole Nationale supérieure des télécommunications Dalloz 1996 Juris p.490

[64] Cap Aix-en-Provence 12 déc. 1996 JCP 1997 . II. 22975

[65] cf Un officier de l'US Navy avait en téléphonant au service technique d'un fournisseur d'accès, sans se présenter ni indiquer le motif de son appel, obtenu le nom et l'adresse d'un de ses membres qui s'était présenté comme homosexuel sur un CV en ligne. " Les mésaventures du sous-marinier McVeigh " Le Monde cahiers multimédia 25, 26 janv. 1998

policiers s'en plaignent). En effet, la commission doit passer par voie diplomatique. C'est la désagréable surprise à laquelle les enquêteurs ont été confrontés dans l'affaire Gigastorage où l'intéressé avait mis sur Internet le dossier d'instruction. Le serveur étant hébergé à Santa Barbara, il fallut passer par les Etats-Unis pour régler l'affaire. Mais les autorités du pays refusèrent l'exécution de la commission rogatoire.

II. LA PREUVE DE L'IDENTITE DE L'AUTEUR

Contrairement à l'idée répandue, il est relativement facile d'identifier l'ordinateur d'où provient un message ou une action car tout ordinateur connecté à Internet laisse son adresse IP[66]. Il est vrai qu'il existe des *remailers*[67] : ces serveurs attribuent à l'internaute qui veut rester anonyme un numéro de série ainsi qu'un mot de passe. Lorsque l'internaute voudra envoyer un message de façon anonyme, il l'enverra sur ce serveur avec l'adresse du destinataire. Le " rerouteur " enverra le message au destinataire en " effaçant " l'adresse IP de l'expéditeur. Mais évidemment, le *remailer* connaît l'adresse de l'auteur.

Une fois l'ordinateur identifié, reste à découvrir quel est celui qui l'a utilisé. Cela peut être très facile si l'ordinateur est la propriété exclusive d'un individu, mais la question se complique lorsque plusieurs individus ont la possibilité d'accéder à un même ordinateur(entreprise, bibliothèque, cybercafé..). Les moyens de preuve traditionnels seront alors employés.

CHAP. 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 sera 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.

SECT°. I. LES EFFORTS DES ETATS

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

§1. LES EFFORTS COLLECTIFS

Favoriser la coopération internationale constitue la troisième piste que le rapport Falque-Pierrotin propose d'explorer.

A. L'ASPECT INCITATIF

[66] pour une démonstration et une explication http://ww.cnil.fr – voir également " Le site DejaNews : un moyen de repérer les criminels opérant dans les forums d'Internet " R. Duncan Bull. sur la criminalité informatique sept. 1997 http://www.rcmp-grc.gc.ca/html

[67] ping@anon.penet.fi - http://www.c².org/remail/by-www.html. – voir aussi " Nuire aux fournisseurs d'information via e-mail :*FakeMail + Spam* " I. Vassileff http://www.grolier.fr/cyberlexnet

M. Fillon avait proposé au Conseil des Ministres des Télécommunications de Bologne en 1996[1] de prendre des dispositions internationales en ce qui concerne :

- les principes minimaux de déontologie applicables aux services sur Internet
- les principes de responsabilité communs aux éditeurs et services d'hébergement
- les principes de base d'une coopération judiciaire
- la détermination des règles applicables

Il serait temps de mettre en œuvre cette coopération.

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 "[2] aura lieu[3]. 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* "[4]. Ce problème a ainsi donné lieu à un certain nombre de communications, résolutions et livre vert relatifs au contenu illégal et préjudiciable sur le réseau Internet[5]. 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[6]. 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 illégaux 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* ".

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 "[7]. 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 "[8].

---

[1] Conseil des Ministres du 24 avril 1996

[2] adoptée par la Commission européenne le 10 déc. 1997

[3] " Préparer l'entrée de la France dans la société de l'information " http://www.culture.fr/

[4] proposition de décision du Conseil faite par la Commission 26 nov 1997 – COM(97) 582 final cons.2

[5] 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

[6] racisme, incitation à la haine ou à la violence, terrorisme, pornographie déviante, négationnisme, exploitation des enfants pour une activité sexuelle selon la Commission

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

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[9].

B. L'ASPECT OPERATIONNEL

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 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[10] a peut-être mis en marche ce mouvement de coopération. Chacun des pays d'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

A. GENERALITES

Alors que certains Etats laissent à Internet la possibilité de " s'épanouir " en toute liberté comme les Pays-Bas[11], 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[12].
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 "[13]. Singapour a étendu les dispositions relatives à la censure des documents à caractère sexuel et a aggravé les peines[14].

B. LE CAS DE LA FRANCE

I. LES PROPOSITIONS DU RAPPORT FALQUE-PIERROTIN

Ce rapport conseille quelques pistes très faciles à mettre en œuvre pour une meilleure appréhension des comportements sur Internet par le droit français. Elles ont d'ailleurs été reprises par un rapport ultérieur.[15]

Il conseille tout d'abord une meilleure connaissance par les magistrats des difficultés que posent Internet. Il est vrai que les juges méconnaissent souvent les dispositions de la loi Godfrain et qu'ils restent

---

[8] 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
[9] " Contenu illégal et préjudiciable sur Internet " rapport intermédiaire 4 juin 1997 http://europa.eu.int
[10] " Les ministres du G8 adoptent un plan d'action contre la criminalité informatique " Le Monde 12 déc. 1997
[11] " Internet, l'Europe et la censure " Le Monde Cahiers multimédia 23, 24 fevr. 1997
[12] Le Monde 8 janv 1998
[13] Le Monde 6 janv. 1998
[14] Le Monde 24 fev. 1998
[15] *Internet et les réseaux numériques* – Conseil d'Etat – Edition de la Documentation française

désemparer devant le réseau. Une circulaire pourrait donc appliquer ainsi rappeler aux parquets le droit applicable. Il serait aussi utile de " *centraliser informations et poursuites à la Chancellerie afin de constituer rapidement un noyau d'expérience et de compétence* ". A ce jour, cette centralisation n'a pas encore eu lieu.
Le rapporteur se demande si la formation de " cyberjuges " est vraiment nécessaire et préfère opter pour la dissémination de la formation à tout l'appareil judiciaire. Les auditeurs de justice effectuent d'ailleurs parfois des stages à la Brigade centrale de criminalité informatique[16] et quelques juges, notamment au parquet de Paris se spécialisent dans la criminalité informatique.

Le rapport préconise également la création d'une nouvelle forme de procédure adaptée à la particularité du réseau. Il s'agirait de créer au profit du Parquet dans le cadre des mesures qu'il peut prendre pour faire cesser toute infraction, une procédure de saisie précédée d'une injonction. L'exigence de cette dernière assurerait une protection de la liberté d'expression.

II. LES PROPOSITIONS LEGISLATIVES

Aucun projet portant sur la création d'une législation spécifique à Internet ne semble envisager. Comme l'a noté le rapport Falque-Perrotin, les dispositions pénales existent, il suffit de les appliquer. Les difficultés qui demeurent devraient par contre faire l'objet d'une législation qui devrait être préparée par le Ministère de la Communication[17].

Mais il est important de souligner à l'instar de la commission du Sénat chargée de l'étude du projet de loi relatif à la délinquance sexuelle[18] que " *loin de marquer le début d'un harcèlement législatif, la répression des abus commis sur l'Internet doit précisément faciliter son entrée dans les mœurs en évitant d'utiliser à des fins illicites, faute de quoi le risque serait grand de voir jeter l'opprobre sur ce procédé et de tenir la France à l'écart de la modernité* ". Le vote de la loi du 17 juin 1998 relative à la délinquance sexuelle a marqué le premier pas dans l'adaptation du droit à l'Internet, qui doit se poursuivre dans d'autres matières.

1. En matière d'audiovisuel

La Commission de l'Assemblée Nationale lors de la première lecture du texte relatif à la protection des mineurs contre la délinquance sexuelle avait également proposé d'adopter des dispositions permettant aux agents du CSA de constater par procès-verbal les infractions prévues aux art. 227-23 et 227-24 CP et d'avertir le Parquet. Elle prévoyait de plus, que si l'infraction était commise via un réseau de télécommunications, ils devaient avertir la personne qui avait offert le " *service de connexion au service de communication audiovisuelle.* ". Le ministre de la Justice demanda à l'Assemblée de ne pas voter cette disposition en précisant que " *toute réforme concernant Internet devrait faire l'objet d'une réflexion d 'ensemble../..et que la proposition de la Commission sera examiné avec une particulière attention par le Gouvernement quand il élaborera cette réforme.* ".

Ainsi, le projet de loi sur l'audiovisuel du 28 janvier 1998[19] reprend cette proposition. Mais il ne sera examiné par le parlement que durant l'automne 1998.

2. En matière de preuve

La Chancellerie envisage de soumettre au Parlement de nouvelles dispositions relatives à la réglementation des perquisitions[20] : Elles autoriseraient les perquisitions de nuit, comme en matière de proxénétisme, de trafic de stupéfiant ou de terrorisme, pour rapporter la preuve de certaines infractions commises via Internet. Les magistrats du Ministère de la Justice avancent le fait que l'utilisation d'Internet se faisant souvent de nuit (car les internautes travaillent dans la journée et parce que les communications sont moins chères).
On peut douter du bien-fondé d'une telle disposition dans la mesure où la preuve de la connexion délictueuse ou du contenu préjudiciel diffusé ou transféré se situe dans le disque dur de l'ordinateur. Nous avons déjà dit que ces informations laissent indéfiniment des traces sur ce disque dur. La perquisition pourrait avoir lieu le lendemain matin que cela ne changerait rien.

[16] interview du commissaire Vigouroux Expertises mai 1995 n°183 p.179
[17] " le contrôle d'Internet " Le Figaro nov. 1998
[18] Rapport de la commission du Sénat n°49 J.O. du Sénat 22 oct 1997
[19] " Les dix vœux du CSA pour la loi sur l'audiovisuel " Le Monde 28 janv. 1998
[20] Entretien avec M. Lagèze Ministère de la Justice – janvier 1998

3. En matière de protection des bases de données

Le Ministère de la Culture a annoncé qu'une loi sera présentée en 1998 pour introduire en droit français la protection des bases de données issue de la directive du 11 mars 1996[21].

SECT°. II. LES EFFORTS DES ACTEURS

[21] " Préparer l'entrée de la France dans la société de l'information " http://www.culture.fr/

Nous ne devons pas oublier qu'Internet est à l'origine un réseau sur lequel règne la plus grande liberté. Les internautes 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 a priori est d'ailleurs la première proposition du Rapport Falque-Pierrotin[1].

§1. LE ROLE DE CERTAINS ACTEURS

A. CONTRE LA FRAUDE INFORMATIQUE[2]

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[3] 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 fait même parfois obligation à certains organismes de protéger les données qu'ils détiennent[4]. 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 sera pas découvert par l'un des logiciels qui peuvent tourner des heures entières pour essayer des mots de passe. Le CERT (*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[5]. Tout d'abord, modifier régulièrement le mot de passe. Une enquête américaine de 1994[6] revèle 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. 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* "[7].

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[8], la violation de ces moyens de protection permettra de plus de rapporter la trace et la preuve des délits.

B. CONTRE LES CONTENUS PREJUDICIABLES

I. L'INFORMATION

[1] *Internet – enjeux juridiques* Rapport Falque-Pierrotin Documentation Française 1997
[2] " Introduction à la sécurité sur l'Internet " Rapport du SCSSI n°2133/SCSSI/SI 12 déc 1997
[3] instruction n°8192/DEF/CAB/CM/3 – BOC/PP 24 mars 1997 n°13
[4] sous peine de sanctions pénales : art. 226-17 CP
[5] *Le monde Internet* Ed. Krol (traduction P. Cubaud & J. Guidon) coll. Guide & Ressources éd. O'Reilly international Thomson 1995
[6] P. Rosé " Délinquance informatique, inforoutes et nouvelle guerre de l'information " - Cahiers de la Sécurité Intérieure n°24
[7] Anthony-Chris " Frantic " Zboralski dans " Cyberwars : la montée du crime informatique " Les Echos 10 fev 1998
[8] " Aspects de la criminalité et de la délinquance en France en 1995 " Ministère de l'Intérieur La Documentation Française

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[9]. 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[10].

II. LES LOGICIELS DE FILTRAGE

Les logiciels de filtrage[11] 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 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, que la seconde méthode ne peut pas rectifier 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[12].

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

[9] 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
[10] comme la police belge http://www.gpj.be
[11] " Censorware, la censure privatisée " Le Monde Cahiers multimédia 12, 13 oct. 1997
[12] Le Monde 1er nov. 1997 - 24 janv 1998

- 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 ?

III. LES CONTRATS

Comme le fait remarquer le rapport Falque-Perrotin, " *les contrats peuvent donner une base légale à un filtrage du contenu* ".
Le contrat[13] peut être un outil de prévention : à défaut de rendre responsables pénalement les opérateurs et fournisseurs, il peut servir à les responsabiliser. Il aura d'autant plus de légitimité que les règles en auront été acceptées les parties.

L'on peut s'appuyer alors sur deux types de contrats
- le contrat entre l'utilisateur et le fournisseur d'accès par lequel le fournisseur d'accès pourra s'engager à ne pas laisser accès à des serveurs délictueux et l'abonné à ne pas éditer de contenu répréhensible. Les sociétés Calvacom, Internet Way, Imaginet et Francenet prévoient déjà dans leur contrat d'abonnement qu'elles exigeront de leur abonnés qui violeraient les dispositions de la loi du 29 juillet 1881 qu'ils cessent leurs agissements et éventuellement rompront le contrat de prestation.
- le contrat entre les propriétaires des infrastructures de télécommunications avec les fournisseurs de services.

C. CONTRE LA CONTREFAÇON

Pour lutter contre la contrefaçon, et surtout pour assurer la rémunération des auteurs, deux solutions pouvaient être adoptées :

- Un système de perception de taxe à priori comme cela existe en matière de cassettes vidéo : une taxe serait ajoutée au prix du CD-Rom vierge pour rémunérer les auteurs des films , musiques, jeux susceptibles d'être enregistrés.
- Un système d'immatriculation des œuvres. C'est la solution retenue par les professionnels et qui se développe : InterDeposit propose l'identifiant IDDN, la CISAC (Confédération internationale des sociétés d'auteurs et compositeurs) propose un système WorksNet[14].

§2. L'AUTO-REGLEMENTATION

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[15].

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.

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,

[13] Lamy informatique 1997 n°2137 - – " Le droit applicable à Internet : de l'abîme aux sommets " N. Brault http://www.grolier.fr/cyberlex.net
[14] " Au fil du Net " Gaz. Pal. 10, 12 août 1997
[15] Résolution du Parlement du 24 avril 1997, Résolution du Conseil du 17 février 1997, Déclaration de Bonn des 6-8 juillet 1997

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[16] à M. Fillon, alors ministre délégué chargé de la Poste, des Télécommunications et de l'Espace une proposition de charte de l'Internet[17]. Cette charte a été précédée de réfléxions 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, des 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 ait 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 lutte contre la pédophilie via 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[18]. Ces 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, 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[19] qui a 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.

---

[16] " Actualité de la régulation de l'Internet " Y. Bréban Gaz. Pal. 13, 15 avril 1997 p.22 – " Au fil du Net " Gaz. Pal. 25, 26 juin 1997

[17] http://www.planete.net/code-internet

[18] " Un nouveau manifeste du droit de l'Internet " interview de D. Kahn Expertises nov. 1997 n° 209 p.339

[19] 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

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.

CONCLUSION

Les difficultés juridiques que soulève le premier réseau multimédia international, Internet, sont très nombreuses. Les questions relatives au commerce électronique, au droit des contrats, à la propriété littéraire et artistique s'ajoutent à celles étudiées en matière pénale.

Ces dernières sont d'autant plus complexes que, comme nous l'avons vu, la délinquance liée au réseau ne relève pas d'une catégorie particulière : Internet est susceptible de faciliter la commission de la plupart des infractions que le droit incrimine. Il est important de souligner que ces comportements répréhensibles ne sont pas générés par le réseau, au risque de minimiser le fantastique progrès qu'il constitue. Certes, certaines infractions sont caractéristiques du réseau (tel l'accès frauduleux ou l'atteinte aux données), mais toute médaille à son revers et pour le reste, les délinquants n'ont fait que profiter des nouvelles possibilités qui leur étaient offertes comme dans tout secteur de la société : " *Internet est un peu comme la voiture de la bande à Bonnot au début du siècle. C'est un moyen d'aller plus vite et plus loin pour commettre des infractions* "[1].

La nouveauté de la forme qu'emprunte la criminalité ne doit pas impressionner les autorités. Un effort doit être mené vers une prise de conscience que les comportements qui s'expriment via et sur Internet sont soumis au Droit, même si parfois il sera nécessaire de l'adapter aux spécificités du réseau et notamment en adoptant une réponse internationale, tout au moins en ce qui concerne les comportements " universellement répréhensibles ". Les acteurs qui y interviennent ont également un rôle important à tenir dans cet effort, notamment au niveau de la prévention des infractions (codes de bonne conduite, contrôle des contenus…).

Si cet objectif est atteint et qu'il contribue à faire des futures " autoroutes de l'information " des moyens de communication sûrs et des " zones de Droit ", la Justice, comme la plupart des activités humaines, profitera certainement des avantages qu'offre la communication multimédia en réseau.

[1] " Trafic sur la Toile " Le Monde supplément multimédia 21,22 juin 1998