COLLEGE INTERARMEES DE DEFENSE

# QUELS SONT LES MOYENS DE LUTTER CONTRE LA CRIMINALITÉ INFORMATIQUE ?

Mémoire de géopolitique

du chef d'escadron Pierre MEYER

dans le cadre du séminaire

« Les criminalités transnationales »

Directeur : Commissaire Principal Philippe MIGAUX
de la sous-direction antiterroriste
Ministère de l'Intérieur

- Avril 2002 -

« L'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquance »

Doyen Carbonnier[1]

# QUELS SONT LES MOYENS DE LUTTER CONTRE LA CRIMINALITÉ INFORMATIQUE ?

## SOMMAIRE



[1] J. Carbonnier, Sociologie juridique, PUF, 1978, p. 401.

# INTRODUCTION

Dans l'espace dit « virtuel » qui se développe au rythme de l'Internet, apparaissent de nouveaux vecteurs d'accès à la connaissance et au développement commercial[2]. Mais qui dit « nouvelle économie » dit aussi nouvelle criminalité. L'Internet, par le développement des moyens informatiques, est le terrain d'action d'une nouvelle forme de « délinquance assistée par ordinateur », commise par une génération de techno-criminels. Comment les systèmes répressifs nationaux -et plus particulièrement en France- peuvent-ils répondre à cette « cybercriminalité », dont l'évolution est constante, et est fonction de la démocratisation de l'accès à l'informatique et de la globalisation des réseaux ?

Définie comme l'utilisation à des fins criminelles des nouvelles technologies de l'information et de la communication, la criminalité informatique se développe d'autant plus aisément et rapidement qu'elle agit, par essence, en dehors des structures étatiques[3]. Elle présente trois critères : elle est réelle, multiforme, et difficilement saisissable. Son importance oblige désormais à des réactions efficaces, et pour cela quasi-immédiates.

De nombreux motifs obligent à considérer la cybercriminalité comme un enjeu de la sécurité des entreprises, mais aussi des Etats[4]. En matière de sécurité, ces nouveaux besoins ne

---

[2] Tous les secteurs, ou presque, de la vie économique sont désormais largement dépendants des Nouvelles Technologies de l'Information et de la Communication (N.T.I.C.) : la bourse, le secteur bancaire, le contrôle aérien, le téléphone, l'énergie électrique … Autant de domaines qui peuvent être pris pour cibles par la cybercriminalité.

[3] Les télécommunications ne sont pas le seul domaine qui outrepasse les limites d'un Etat national : le trafic aérien, le droit de la mer, les transferts de fonds ou les questions d'environnement ont contraint à des efforts concertés au plan international.

[4] Dans le cadre de cette étude, nous n'abordons pas le cyberterrorisme en tant que tel, puisque nous traitons uniquement des moyens de lutte contre la cybercriminalité au plan juridique, et non selon une thématique criminelle. Des méthodes techniques similaires sont utilisées par toutes les organisations criminelles en matière de délinquance et de criminalité informatique, qu'il s'agisse des domaines financier ou politique. De plus, le cyberterrorisme relève, à notre sens, d'un champ d'étude singulier, qui exige, pour son entière compréhension, une analyse exhaustive, découlant nécessairement d'une appréhension spécifique de ce phénomène.

trouvent pas encore de réponses entièrement adéquates, puisque la délinquance informatique est hors frontière, ce qui rend les investigations d'autant plus difficiles.

Le postulat est que pour lutter efficacement contre la cybercriminalité, le cadre des souverainetés est désormais dépassé. Outre les systèmes de protection privés, qui peuvent être piratés et détournés plus ou moins aisément, les Pouvoirs Publics se trouvent dans l'obligation de répondre aux attentes des entreprises et des banques, et de les protéger en amont des attaques potentielles, comme de les soutenir et de rechercher les criminels en aval, à la suite de telles attaques.

Il s'agit pour cela de définir une mission, celle de l'obtention de la preuve ; de désigner un ou des coordinateurs parmi les organisations nationales et, s'il est possible, transnationales ; et de leur donner les outils, pénaux, financiers et humains nécessaires à cette tâche.

Si des moyens juridiques sont avant tout mis en œuvre contre la criminalité informatique, ils restent toujours accompagnés de leurs corollaires, des moyens techniques.

## PREMIERE PARTIE - DES MOYENS JURIDIQUES : L'OBTENTION DE LA PREUVE

Les principes des régimes démocratiques obligent à l'obtention de la preuve, qui, bien que difficile, passe nécessairement par une coordination des poursuites et l'utilisation d'un arsenal répressif.

### 1.1/ LE MYTHE DU VIDE JURIDIQUE

Non seulement Internet ne représente pas en la matière un vide juridique, mais encore la régulation de ce réseau même est encombrée d'une quantité respectable de normes applicables, peut-être redondantes. En effet, plusieurs droits s'appliquent au Net : le droit de l'audiovisuel, celui de la presse, de la télématique, … En France, le régime juridique de l'Internet relève pour l'essentiel du droit de la communication audio-visuelle. [5] Pour le

[5] Article 2 de la loi du 30 septembre 1986.

Conseil d'Etat[6], un droit sectoriel spécifique au Net ne paraît pas nécessaire, car c'est le type de cybercriminalité qui doit déterminer, au cas par cas, le régime juridique applicable. Les conclusions de la Commission européenne sont similaires, incluant toutefois un complément quant au statut des fournisseurs d'accès, et à l'obligation de territorialisation des sites des fournisseurs. L'ensemble de la législation existante a vocation à s'appliquer aux acteurs d'Internet, notamment les règles de procédure de la vie privée et du consommateur, et celles qui garantissent le respect de l'ordre public. Dans l'espace des réseaux, tout type d'activité peut être pratiqué dans le respect des règles de droit commun, qui régissent un domaine spécifique : publicité, fiscalité, propriété industrielle, propriété intellectuelle … Quitte à l'adapter, le corpus de textes existant peut être appliqué à l'ensemble des activités existantes sur Internet.

Néanmoins le Net oblige peut-être à élaborer une nouvelle classification du droit civil. Ainsi en est-il en matière du droit de la preuve.[7] En droit pénal, de même, de grandes incertitudes apparaissent quant à la détermination d'un régime unique de responsabilité des acteurs, mais aussi quant à l'application potentielle d'un droit pénal spécifique aux réalités techniques.

Avant d'aborder la question même du droit applicable, il apparaît utile de rappeler l'existence du principe de proportionnalité, qui détermine, en France, les conditions d'application des règles de lutte contre la cybercriminalité, en déterminant un cadre législatif d'action policière, judiciaire, et pénale. Ce principe énonce que toute limite, justifiée par un motif d'intérêt public, à l'exercice par les citoyens des libertés publiques, doit être strictement proportionnelle à l'objectif à atteindre. Applicable par le juge en l'absence même de texte[8], il a été étendu aux applications de l'informatique, et est mis en

[6] Dans un rapport au Premier ministre, rendu en 1998. Ce rapport est publié à la « Documentation française », et est disponible sur Internet sur le site http://www.internet.gouv.fr/français/textes-ref/rapce98/accueil.htm.

[7] La progression de l'utilisation du courrier électronique conduit à repenser la tradition juridique française de l'écrit comme preuve singulière. En droit des contrats de même, la question se pose quant au moment de la conclusion du contrat électronique.

[8] Le Tribunal administratif de Marseille a rappelé en l'espèce que le principe de proportionnalité est applicable sans texte, mais il n'est pas pour autant interdit de fixer par dispositions écrites des outils juridiques, afin

œuvre par des dispositifs législatifs spécifiques, rattachés aux textes de la filiation « Informatique et Libertés ».

Ce principe trouve son fondement juridique dans l'article 8 de la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale publiques ou à la protection des droits et libertés d'autrui ».

La question est celle de la justification de la restriction des libertés au profit d'une action de police, et donc de concilier des intérêts a priori opposés. Si le champ des intérêts protégés est ici délimité, les logiques de l'action publique sont quant à elles nombreuses, mais peu précises. Dans une société démocratique, et selon l'article 8 énoncé plus haut, la sécurité nationale doit être remise en question pour que puissent être outrepassées les libertés privées.

Le principe de proportionnalité provient de cette recherche nécessaire d'un équilibre. En France, s'établit depuis plus de vingt ans un corpus de règles applicables au traitement des informations, directement ou non nominatives. Ce corps est constitué de la loi du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et de la convention 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des données à caractère personnel[9].

Depuis le milieu des années quatre-vingt dix, le Conseil constitutionnel comprend la loi du 06 janvier 1978 comme partie du socle des lois de libertés publiques, dont la

---

d'aider les acteurs publics qui jugent des recours aux nouvelles technologies de l'information et de la communication (N.T.I.C.) comme atteintes aux libertés et à la vie privée.

[9] En vigueur depuis le 1er octobre 1985.

Constitution -et le bloc de constitutionnalité- garantit la pérennité. La vie privée est alors entendue comme une composante majeure de la liberté individuelle. De plus, la loi de 1978 a un caractère d'application générale, et peut en conséquence être écartée par le législateur au profit de régimes juridiques autonomes, sous le contrôle du Conseil constitutionnel. Mais la dérogation doit alors être expresse[10].

Le principe de finalité est le premier des principes de protection des données : un traitement de données doit avoir une finalité précise et déclarée par son responsable. Des principes corollaires concernent la nature et la masse des données, leur durée de conservation, les destinataires, et l'usage qui en est fait. Les données doivent être « adéquates, pertinentes, et non excessives » selon la finalité du traitement. Parmi ces données, certaines plus délicates jouissent d'un statut spécifique, et concernent les domaines d'appartenance religieuse ou philosophique, ceux relatifs aux opinions politiques, aux appartenances syndicales et ethniques, à la santé, aux mœurs et à la vie sexuelle. Ces données, sauf dérogation pour motif d'intérêt public, ne peuvent faire l'objet d'un traitement automatique qu'après consentement exprès de la personne concernée. [11]

[10] Ce fut le cas pour la loi du 21 janvier 1995, qui encadre le recours aux systèmes de vidéo-surveillance dans les lieux publics et les lieux privés ouverts au public.

[11] Il en est ainsi du N.I.R. (numéro d'inscription au répertoire national des personnes physiques), dont l'utilisation est subordonnée aux décrets du Conseil d'Etat, pris après avis de la C.N.I.L.. Il en va de même pour les infractions, les condamnations, et les mesures de sûreté, qui ne peuvent être traitées que dans le fichier d'un service relevant du ministère de la Justice (le casier judiciaire).
Les modes de contrôle et d'intervention de la C.N.I.L. doivent évoluer afin que l'informatique ne permette pas ce que le législateur a voulu interdire. L'interconnexion des fichiers peut rester l'exception, et correspondre de même à une vigilance propre à l'utilisation et à la diffusion du N.I.R. L'action de la police, tiers autorisé, est plus que nécessaire. La C.N.I.L. prône de son côté une grande transparence, et garantit un accès indirect aux fichiers.

Le dernier principe, mais non des moindres, qui protège les libertés individuelles[12] et limite les actions publiques, est celui de la non automaticité des décisions, prévu par la loi de 1978, et qui ne conçoit pas que l'être humain puisse être traité à l'égal d'un objet. Le résultat du traitement informatique ne doit donc pas être appliqué mécaniquement, mais une appréciation humaine apparaît indispensable à une prise de décision à l'encontre de quelqu'un. La loi de 1978 réfute également les décisions administratives prises selon des profils de personnalité.

Le principe de proportionnalité se propose de contenir les excès et dérives de l'informatique, et cette question détermine le cadre d'action des Pouvoirs Publics dans la lutte contre la cybercriminalité, qui oblige à des recherches et des contrôles informatiques, touchant par essence aux libertés individuelles : adresses privées, dénominations, surveillance… [13]

La confrontation du droit et de l'informatique, en particulier du Net, oblige à prendre en considération de nombreuses données techniques pour pouvoir comprendre la volonté et le processus criminels. En effet, deux types de criminalité informatique apparaissent : la cybercriminalité pour laquelle Internet et l'informatique en général sont des supports de l'action criminelle, et celle où le Net constitue le moyen même, au sens d'outil, de la criminalité. Il convient de ne pas confondre ces deux types de situations : la commission de délits classiques au moyen de l'informatique, et les cas où l'informatique est le but même de la cybercriminalité. En effet, les réponses répressives varient du tout au tout selon ces situations.

---

[12] Le bogue de l'an 2000 a sensibilisé à la vulnérabilité des systèmes informatiques, au delà même des pertes financières, au plan des libertés fondamentales. Une nouvelle vulnérabilité apparaît, qui découle de la complexité des systèmes, de leur incohérence, et des facteurs humains. Des évaluations globales des systèmes informatisés devraient être systématisées, et correspondre au développement d'une éducation à la vulnérabilité. Les acteurs du Net doivent cesser de croire en l'illusion d'une sécurité propre aux N.T.I.C.

[13] Dans la lutte contre la cybercriminalité, ne sera pas abordée la question du respect de la règle par les autorités publiques. Le sujet est limité à la criminalité privée, et ne concerne en rien les actions illégales qui pourraient être commises par des autorités publiques. Le respect de la règle par l'autorité est un autre sujet, celui de l'« enforcement », terme anglo-saxon qui désigne des mécanismes de surveillance.

Dans le cas de la cybercriminalité en tant qu'instrument de la commission de délits classiques, l'application des textes pénaux existants à l'informatique et aux réseaux ne pose pas de problème, sous réserve des difficultés inhérentes à l'identification des auteurs, et aux poursuites des infractions commises depuis des serveurs étrangers. Ces difficultés résultent de l'essence même du réseau Internet, international et décentralisé.[14]

Cette cybercriminalité joue sur un terrain favorable, où elle peut développer des opportunités lucratives, à partir de vieilles techniques criminelles : introduction de virus ou de bombes logiques afin de perturber un système informatique, ce qui constitue un moyen de chantage ; modification de programmes comptables pour détourner des fonds ; contrefaçon d'œuvres protégées, facilitée par l'utilisation de logiciels. De plus, l'utilisation du système technique des cartes bancaires permet la fabrication frauduleuse de cartes à partir d'un numéro de compte existant ou fictif, en vue d'escroqueries ; la proposition sur Internet de marchandises ou de prestations fictives, payées avec de vraies cartes ; et la fabrication de cartes à puces pour tromper les terminaux de paiement, en acceptant toutes les transactions quel que soit le numéro de code secret tapé par le porteur.

A ces anciennes techniques criminelles, pour lesquelles l'informatique est un outil comme un autre, le droit pénal répond le plus souvent. Mais pour quelques rares cas, en raison des termes légaux utilisés, l'application au cyberespace de certains textes pénaux anciens s'avère délicate. Le vol de données informatiques en est un bon exemple, dans la mesure où le fait de subtiliser des fichiers informatiques en les copiant n'implique pas en principe, selon l'acception courante, une soustraction frauduleuse du corps du fichier. Or c'est là l'élément constitutif du vol. Ainsi la jurisprudence, pour pouvoir conclure au vol, a dû élaborer une construction juridique spécifique et audacieuse, décidant en la matière que cette soustraction frauduleuse pouvait apparaître du simple fait de priver autrui de l'exclusivité de la possession juridique

[14] En France, un jugement du 16 février 1998 du Tribunal correctionnel du Mans a condamné l'ancien directeur de cabinet du Président du Conseil général de la Sarthe à trois mois de prison ferme pour recel d'images pornographiques de mineurs, stockées sur le disque dur de son ordinateur après téléchargement depuis des sites web.
Dans une autre affaire, par décision du 27 août 1999, une personne a été condamnée par le Tribunal correctionnel de Strasbourg pour avoir exprimé des propos racistes dans un forum de discussion.

d'un bien, par l'effet de la copie. La copie de fichier peut donc être interprétée comme une atteinte au principe de la propriété privée, mais une jurisprudence a été nécessaire à ce résultat.

De même, en matière de jeux de hasard sur Internet, ou de « casinos virtuels », se pose un problème épineux d'interprétation de la loi pénale, dans la mesure où le Code pénal vise le délit de tenue de « maison de jeu » de hasard, et que la référence à un « bâtiment » ou «édifice » n'apparaît pas possible, parlant d'un site Web[15]. Le seul recours aux règles d'interprétation évolutive de la loi pénale, définies strictement par la Cour de cassation, pourrait permettre d'étendre la prohibition de tenue de maison de jeu aux casinos virtuels. Mais la question demeure encore, pour partie, à l'étude.

L'informatique est donc devenue une cible, et depuis son émergence Internet a connu un essor remarquable de la criminalité informatique. En France, en 1996, 161 enquêtes pénales ont été ouvertes, 424 en 1997, et 564 en 1998 … Ces ouvertures d'enquêtes constituent, de plus, une portion infime du nombre des fraudes informatiques, car les victimes de ces fraudes préfèrent souvent garder le silence, en particulier pour ne pas perdre leur crédibilité auprès de leurs clients. De plus, certains logiciels en accès libre sur le Net, peu complexes d'utilisation, permettent par exemple de créer de faux numéros de cartes bancaires, ou bien encore de modifier la page d'accueil d'un site Web. [16]

Les procédés cybernétiques du Net peuvent bien constituer une arme car ils permettent de détruire et de conquérir, et non seulement de diffuser. Cette utilisation, plus « active », sert des fins tactiques, et diffère de celle où l'informatique joue un rôle passif d'information. La cybercriminalité n'est pas limitée à l'utilisation d'Internet à des fins criminelles, et correspond aussi au Net comme objet criminel.

Au-delà de manifestations topiques d'individus privés commettant des délits sur le Net, à petite échelle, d'une manière amusante et certes efficace, il existe de fait une

[15] Ensemble de textes, de logiciels, et d'applications stockés sur le disque dur d'un serveur.

[16] En 1984, le « Canard Enchaîné » démontrait déjà qu'au moyen d'un minitel, quelqu'un possédant un minimum de connaissances techniques pouvait obtenir nombre d'informations sur les projets nucléaires français, en pénétrant les réseaux des administrations et des entreprises du secteur.

cybercriminalité organisée, plus insidieuse, plus discrète, et ainsi plus à l'abri. Si la cybercriminalité touche tous les secteurs, privés comme publics, la répression doit demeurer publique, car elle touche à l'un des pouvoirs régaliens de l'Etat.

La réponse pénale à la cybercriminalité est contenue dans la criminalisation des infractions informatiques, longtemps considérées comme des infractions ordinaires, qui viseraient une catégorie particulière de biens. C'est le développement de la criminalité informatique et l'augmentation continue des crimes en réseau qui ont rendu nécessaire l'adoption de dispositions pénales particulières, qui prennent en compte la dimension technique de ce nouveau sujet d'étude de la criminalistique. [17]

En France, la loi Godfrain[18], reprise dans le Nouveau Code pénal sous les articles 323-1 et suivants, définit les enjeux de la sécurité informatique. L'arsenal juridique est ainsi formé de trois délits distincts, qui visent les atteintes aux systèmes et les atteintes aux données de quelque sorte qu'elles soient.

De fait, les qualifications juridiques des faits sont particulièrement difficiles, plus spécifiquement celles qui concerneraient les phénomènes d'intrusion et les attaques logiques. En l'absence d'une jurisprudence suffisante, de nombreuses incertitudes demeurent quant au contenu réel des incriminations potentielles.[19] Enfin, la complexité technique de la mise en place par étapes du piratage pousse au constat de concours réels d'infractions.

---

[17] La première loi qui concernait directement la cybercriminalité et la répression de la cyberdélinquance fut adoptée aux Etats-Unis. Il s'agit du Comprehensive Crime Control Act en 1984, amendé par le Computer Fraud and Abuse Act en 1986. Ils criminalisent plusieurs types d'accès frauduleux aux systèmes informatiques, selon la finalité de l'acte d'intrusion réalisé :

-obtention d'informations sur des secrets d'Etat ou injure aux Etats-Unis

-vol de données financières confidentielles

-visite d'un ordinateur appartenant à une administration fédérale

-accès frauduleux à un ordinateur avec une intention d'y commettre des méfaits informatiques

-trafics de mots de passe, lorsqu'ils affectent le fonctionnement du commerce extérieur

[18] du 05 janvier 1988.

## 1.2/ DES FAITS AUX PREUVES : L'ARSENAL REPRESSIF

L'arsenal répressif français détermine les éléments de la preuve selon les infractions.

1.2.1/ Ainsi, l'intrusion ou le maintien frauduleux dans un Système de Traitement Automatisé de Données (S.T.A.D.) est puni, selon l'article 321-1 du Code pénal, d'un an d'emprisonnement et d'environ 15 244 Euros d'amende. Deux éléments de qualification sont retenus.

Tout d'abord, l'élément matériel : la pénétration ou le maintien dans un système.

La pénétration d'un système revêt différentes formes, qui correspondent à autant d'options techniques. « L'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de télécommunication »[20].

Toutes les actions d'intrusion directe relèvent, ou peuvent relever, de ce chef d'incrimination, et le simple acte de pénétration est ainsi en soi-même répréhensible. La difficulté relève alors de l'établissement de l'élément matériel, et en particulier lorsque aucune modification des données n'a été effectuée par le pirate. De la même manière, l'utilisation d'un mot de passe frauduleux, comme d'une fausse identité, est, bien entendu, à comprendre comme un mode de pénétration parfaitement irrégulier.

Le maintien dans un système est l'une des conséquences d'un accès interdit, et concerne tout autant un maintien frauduleux à la suite d'un accès licite : lorsque, par exemple, l'auteur de l'infraction est « privé de toute habilitation » à utiliser les ressources du système pénétré. [21] La même procédure s'applique lorsque l'auteur de l'infraction

---

[19] A l'exemple de l'introduction d'un programme sniffer : TGI Paris, 16 décembre 1997, Actualité Lamy, droit de l'Informatique, mars 1998, p. 1 à 3.

[20] Paris, 05 avril 1994.

[21] Paris, 05 avril 1994.

comprend cette absence d'habilitation à la suite d'un accès involontaire au système propre, soit après une intrusion « par erreur », et même sans volonté frauduleuse.

Ensuite, l'élément moral : la volonté frauduleuse.

Au sens de l'article 323-1 du Code pénal, qui définit l'intrusion informatique et sa répression, elle doit être délibérément voulue par un auteur, qui a conscience de ses actes et de leur irrégularité lorsqu'il commet cette infraction. L'accession à des sites Web payants, ou à accès restreint, d'une manière frauduleuse[22] par des hackers est répréhensible en fonction du degré de connaissance informatique de l'auteur et de sa connaissance du fonctionnement de l'Internet. C'est la conscience de l'irrégularité de l'acte (accéder frauduleusement au système) qui détermine la peine. Mais la personne qui utilise le mot de passe falsifié, et celle qui l'a découvert ou inventé ne relèvent pas de la même logique répressive.

1.2.2/ Les atteintes au fonctionnement (entraver ou fausser) d'un S.T.A.D. sont réprimées par l'article 323-2 du Code pénal, de trois ans d'emprisonnement et de près de 45 000 Euros d'amende. En matière d'attaque logique, l'incrimination concerne principalement l'introduction volontaire, dans un système, de virus ou de bombes logiques.

L'introduction d'un élément logiciel corrupteur qui entraînerait un sinistre informatique doit nécessairement être volontaire. Cette logique formelle exclut les transmissions automatiques de fichiers virus par courrier électronique.[23] De même, le caractère intentionnel du délit s'oppose à la répression des communications de fichiers corrompus par des virus à l'insu de l'auteur.

L'acte incriminé doit avoir un effet sur la capacité de traitement de la machine, bien que le degré de perturbation des opérations de traitement importe peu. L'entrave au fonctionnement, ou le faussement d'un système, concerne toutes les hypothèses de

[22] Par une porte d'accès préalablement piratée « backdoor », ou par l'utilisation de mots de passe frauduleux et d'une fausse identité pour accéder au service, en trompant les dispositifs d'identification.

paralysie ou de ralentissement de ce système informatique. La Cour d'appel de Paris a adopté une interprétation large de ce texte[24], en estimant que « de simples effets perturbateurs (…) ayant entraîné un ralentissement de la capacité » du système, ce fait justifie l'application de l'incrimination. Mais il semble que l'introduction de virus aux effets bénins relèverait plus aisément de l'article 323-3, sous la qualification d'introduction frauduleuse de données.

1.2.3/ Les atteintes volontaires aux données relèvent, quant à elles, de l'article 323-3 du Code pénal, qui les punit de trois années d'emprisonnement et de 45 000 Euros environ quiconque aura frauduleusement introduit, supprimé ou modifié les données contenues dans un S.T.A.D.

Apparaît ainsi la notion de données protégées : tout programme, défini comme un ensemble organisé de données en vue d'accomplir une tâche informatique précise, est sujet de la protection pénale prévue, au même titre que tout fichier. Cette protection s'étend au support physique des données protégées. Au sens de la loi Godfrain, la notion de système est extensive et permet de reconnaître comme partie d'un S.T.A.D. les bandes magnétiques, les disquettes, et tous autres matériels et périphériques de stockage, même temporairement reliés au système protégé. L'interprétation jurisprudentielle de l'incrimination protège aussi bien les données non encore entrées dans le système, mais simplement destinées à y être intégrées. [25]

La nature des atteintes concerne l'introduction, la suppression, ou la modification des données. D'une manière usuelle, cela concerne plus l'écrasement de données stockées ou leur déplacement, et il paraît difficile de saisir la distinction voulue par le législateur entre ces deux opérations concomitantes, et même identiques. Pour modifier des données, il faut en effet en retrancher des portions ou les déplacer.

---

[23] Un virus informatique prendrait ainsi furtivement le contrôle de la messagerie de la victime, et se propagerait en envoyant automatiquement des courriers électroniques à toutes les personnes référencées sur le carnet d'adresses.

[24] Op. cit, 05 avril 1994.

[25] Par une décision du 05 janvier 1994, la Cour de cassation a affirmé la constitution du délit alors que la modification d'une donnée avait été faite (un taux de T.V.A.) sur une fiche manuscrite par la suite entrée dans le système. (Cass. Crim., 05 janvier 1994, JCP éd. E., 1994, I, 359, obs. Vivant et Le Stanc).

1.2.4/ L'association de malfaiteurs informatiques, enfin, est visée à l'article 323-4 du Nouveau Code pénal, et réprime, en tant que délit distinct des précédents, la participation à un groupement formé ou à une entente établie en vue de la préparation d'un délit informatique. L'ambiguïté du texte, qui repose sur la notion, d'acception large, de « groupement », ne gêne pas en l'occurrence, car le groupement peut être aussi bien une entité structurée juridiquement ou plusieurs personnes physiques assemblées pour un même but. Ni la forme du groupement ni sa taille n'importe à l'application du texte.

La réalisation matérielle de l'infraction réside, outre la réunion, dans la coopération des membres aux fins de mener à bien le processus criminel. Les hackers s'échangent des informations précises et exploitables sur Internet en vue de casser des codes machine ou de violer des systèmes de sécurité. Cette coopération active est visible et très ouverte dans de nombreux groupes de discussion, aisément accessibles. Mais peut-on pour autant considérer que tout hacker, même agissant seul, répond de cette logique d'association de malfaiteurs ? La réponse de la Cour est affirmative, qui retient l'association de malfaiteurs sur la seule base d'informations échangées, mais indispensables à la pénétration du système informatique. Cette coopération relève peut-être plus de la notion de complicité par instigation ou par fourniture de moyens.

Il demeure une question plus délicate, celle de la responsabilité du site hébergeur, question qui dépendrait d'un jeu de responsabilités, selon un principe de responsabilité en cascade, propre aux infractions de presse [26]. Le rapport publié par le Conseil d'Etat en 1998 « Internet et les réseaux numériques » jugeait ce principe inadapté au Net, en raison de la multiplicité de ses acteurs, dont la spécificité s'accorde mal avec les catégories légales. Pour l'heure, la responsabilité pénale des hébergeurs, à la suite de nombreux et houleux débats juridiques et d'opinion publique, est cantonnée au seul cas où, ayant été averti par l'autorité judiciaire de l'existence d'un contenu illicite présent sur ses serveurs, le

[26] Internet dépend pour l'heure du régime juridique de la communication audiovisuelle, définie à l'article 2 de la loi du 30 septembre 1986 : « la 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 qui n'ont pas le caractère de correspondance privée ».

fournisseur de services d'hébergement n'aurait pas collaboré, et maintiendrait la mise à disposition du public de contenus illicites. [27]

Dans son rapport au Premier ministre, le Conseil d'Etat a défini le régime de lutte applicable au Net. Il porte sur trois points.

Il expose tout d'abord des recommandations générales de coordination interministérielle des positions françaises dans les négociations internationales, concernant Internet et les réseaux numériques, et d'institution d'un dispositif de veille et d'observation juridiques de ces réseaux.

Il est, pour lui, nécessaire de protéger les données personnelles et la vie privée, en adaptant et en renforçant le rôle de la C.N.I.L. : suivi des procédés d'auto-régulation, contrôle a posteriori des pratiques des acteurs. Il apparaît de plus aux juristes du Conseil d'Etat la nécessité d'un accord international, qui fixerait des principes déontologiques communs pour la collecte et l'utilisation des données personnelles.

Néanmoins sa plus longue recommandation concerne le commerce électronique, pour lequel les échanges doivent être favorisés par une confiance accrue des acteurs. Le consommateur doit être protégé par une clarification du régime juridique de la transaction électronique, une meilleure information, et une adaptation de la loi du 04 août 1994 sur l'emploi de la langue française en cette matière. Il faut de plus définir par une convention internationale un socle minimal de principes relatifs à la protection du consommateur, et reconnaître dans le code civil la valeur juridique du document et de la signature électroniques. L'usage de la cryptologie doit être libéralisé, et il faut adapter le régime de la T.V.A. et de l'impôt sur les sociétés aux spécificités des réseaux numériques, et créer de nouvelles formes de recouvrement des taxes sur le Net. Le régime du droit d'auteur devrait être adapté dans un cadre international, plus précisément en matière de « copie privée », et en maintenant un niveau de protection convenable des auteurs. La dernière recommandation générale porte sur le renforcement de la lutte contre la contrefaçon sur les

[27] Loi de 1986 sur la liberté de communication audiovisuelle ; amendements, en mai 1999, au projet de loi portant réforme de la loi de 1986 ; loi du 01 août 2000 ; directive européenne du 17 août 1999 sur le commerce électronique ; décision n° 2000-433 DC du 27 juillet 2000 du Conseil constitutionnel, qui invalide certaines dispositions de l'article 43-8 de la loi d'août 2000.

réseaux, par une coopération accrue des acteurs et par une adaptation de la procédure judiciaire.

Il définit ensuite, d'une manière large, la lutte contre les contenus illicites et les comportements illégaux sur le Net. Il s'agit alors de clarifier le régime de responsabilité des différents acteurs du Net, d'adapter la procédure judiciaire pour faciliter les poursuites, et de renforcer les pouvoirs du juge. Parallèlement il serait bon de créer un pôle interministériel pour la criminalité de haute technologie. Et de renforcer, en la simplifiant, la coopération internationale en matière d'entraide judiciaire, tout en développant l'auto-régulation des acteurs par la création d'un organisme de « corégulation ».

Enfin, il préconise d'adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications, en maintenant la distinction entre le régime de la communication au public et celui de la correspondance privée. La réglementation doit être adaptée pour tenir compte des effets de la convergence : il faut maintenir une réglementation sectorielle pour les services offerts au public, mais uniformiser les règles applicables, progressivement, aux différents réseaux de télécommunication. Enfin, la loi doit définir un socle minimal d'obligations applicables à toute communication au public : protection des mineurs ; respect de la dignité humaine, de la vie privée, des données personnelles, de la propriété intellectuelle ; identification de la publicité comme telle ; …

Outre la création d'incriminations spécifiques aux infractions et délits informatiques, ont été créées des cellules de réflexion et des unités spéciales de police, de gendarmerie et des douanes pour lutter contre les criminels informatiques. Les différentes formes de criminalité sur le Net, et leur progression, démontraient l'échec des systèmes de contrôle étatiques et des instruments classiques de lutte contre la criminalité. Ces forces appliquent un nouvel arsenal juridique, mais participent aussi d'un nouvel élan de coopération internationale de lutte contre la cybercriminalité, qui, essentiellement, contrevient au développement du commerce

électronique et aux bonnes mœurs, donc à la jouissance « en bon père de famille » du Net comme instrument de communications, de services, et d'échanges.

Les Pouvoirs Publics français doivent renforcer le dispositif de coordination interministérielle, de manière à faire travailler de concert administrations et acteurs privés, afin que la France puisse peser réellement sur l'issue des négociations internationales continues.

## DEUXIEME PARTIE - DES MOYENS TECHNIQUES : VERS UNE ORGANISATION TRANSNATIONALE

En sus des organisations et des services nationaux de lutte contre la criminalité informatique, sont peu à peu définies des réglementations européennes et des instances de coopération transnationales, plus qu'internationales.

### 2.1/ L'UTILISATION DES INSTANCES ACTUELLES

Les services de lutte contre la criminalité informatique sont essentiellement d'ordre judiciaire, mais d'autres administrations en France participent de cette lutte.[28]

Il est nécessaire de bien comprendre l'impact des nouvelles technologies, et les objectifs à protéger : le patrimoine, l'intelligence économique, la lutte contre les attaques aux intérêts fondamentaux de la nation, pour organiser une riposte juridique et physique, mettant en œuvre une veille, et des structures préventives et répressives, et autant que faire ce peut en dehors du territoire national.

2.1.1/ Les organes de police judiciaire spécifiques à cette lutte ont été mis en place à la suite de la loi Godfrain du 05 janvier 1998, qui réprime les atteintes aux systèmes de traitement automatisés de données, et qui complète le Code pénal. La police judiciaire française a alors été dotée de deux nouveaux services spécialisés dans la lutte contre la délinquance informatique.

[28] Notamment par l'accès de toutes les institutions policières à des bases de données, qui puissent être consultées et alimentées. Par exemple, le Système de traitement des infractions constatées (S.T.I.C.), et non plus de l'information criminelle, depuis l'intervention de la C.N.I.L.

La Brigade centrale de répression de la criminalité informatique (B.C.R.C.I.), qui dépend directement de la Direction centrale de la police judiciaire. Cette unité est opérationnelle depuis le mois de septembre 1994, et connaît une triple mission : elle assure le soutien des services régionaux de police dans la résolution d'affaires ayant trait à son domaine d'action ; elle collabore avec les organismes de lutte à caractère international, dont, avant tout, ceux d'Interpol ; elle mène ses propres enquêtes, à caractère souvent transfrontalier.

Le Service des enquêtes sur les fraudes aux technologies de l'information (S.E.F.T.I.) a été créé par le préfet de police Massoni le 11 février 1994, et dépend de la sous-direction des affaires économiques et financières de la Direction de la police judiciaire de la préfecture de police de Paris. Sa compétence est territoriale, limitée à la ville de Paris, aux départements adjacents de la Seine-Saint-Denis, du Val-de-Marne et du Val-d'Oise. Souvent présent dans les colloques d'information et de prévention, le S.E.F.T.I. remplit une mission pédagogique, et informe les organismes privés et publics susceptibles d'être victimes de fraude informatique. Il apporte enfin son concours aux enquêtes, grâce aux outils informatiques dont il dispose.

La Direction de la Surveillance du Territoire (D.S.T.) mène de la même manière une action de surveillance des activités cybercriminelles, dans le cadre de sa mission de protection des atteintes aux intérêts fondamentaux de la nation, par le biais d'un service spécifique aux questions informatiques, créé dès 1986. [29] Ses activités, discrètes par essence, sont de trois ordres.

Tout d'abord, renseigner le gouvernement quant à l'évolution des phénomènes de cybercriminalité.

Ensuite, sensibiliser les administrations et les entreprises concernées quant aux risques techniques encourus.

Enfin, agir dans un cadre judiciaire si le domaine de compétence de la D.S.T. est concerné.

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication a été créé par le décret n° 2000-405 du 15 mai 2000. Dépendant de la Direction centrale de la police judiciaire et de la sous-direction des Affaires économiques et

[29] Décret du 22 décembre 1982.

financières, ses domaines de compétence concernent les infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication et les infractions dont la commission est facilitée ou liée à l'utilisation de ces technologies. Cet office connaît plusieurs missions.

Il coordonne la mise en œuvre opérationnelle de lutte contre les cybercriminels.

Il procède, à la demande de l'autorité judiciaire, à tous les actes d'enquêtes et de travaux techniques d'investigations, en assistance aux services chargés d'enquêtes de police judiciaire sur ces infractions.

Il apporte, à leur demande, une assistance aux services de police, de gendarmerie, de la Douane, de la Direction Générale et du Contrôle de la Concurrence et de la Répression des Fraudes (D.G.C.C.R.F.), en cas d'infractions liées à ces technologies.

Il intervient d'initiative, avec l'accord de l'autorité judiciaire saisie, pour s'informer sur place des faits relatifs aux investigations conduites.

2.1.2/ D'autres administrations participent de cette lutte contre la cybercriminalité.

Le Département informatique et électronique de l'Institut de recherche criminelle est une section d'investigation, qui dépend directement de la gendarmerie nationale, et a été créé en 1990. Il est installé à Rosny-sous-Bois, et effectue des expertises dans le cadre d'enquêtes de police judiciaire menées par la gendarmerie. Une section spécialisée assure les fonctions d'analyse criminelle dans la résolution des délits qui impliquent notamment l'informatique et les réseaux du Net. Cette brigade est plus spécifiquement en charge des affaires de pédophilie. Cet institut possède également une section de formation de techniciens spécialisés.

Les services des douanes comprennent une cellule Traitement du Renseignement et Action contre les Circuits Financiers (T.R.A.C.F.I.N.), créée par le décret du 09 mai 1990, et qui remplit une mission de coordination des services en matière de lutte contre le blanchiment de capitaux et le transfert de fonds occultes et illicites. Elle opère à ce titre une surveillance des virements électroniques de fonds qui sont facilités par l'Internet et les réseaux numériques.

2.1.3/ La cryptologie demeure à ce jour le moyen unique de sécuriser les correspondances sur le Net, et il fait l'objet d'un important débat en matière de législation : la sécurité, qui peut

relever d'une prérogative étatique, mais aussi d'un droit individuel, est l'enjeu premier du statut de la confidentialité dans les sociétés de l'information[30].

Si le gouvernement américain[31] est le premier à avoir voulu élaborer une régulation de l'usage de la cryptographie asymétrique[32], à ce jour le seul exemple de mise en œuvre légale du système de dépôts des clefs privées est la loi française du 26 juillet 1996. Jusqu'en 1990, la cryptographie était demeurée en France soumise au décret-loi du 18 avril 1939 relatif aux

[30] Lors de son intervention du 15 octobre 1997 devant l'Assemblée générale des Nations Unies, le Président des Etats-Unis de l'époque, Bill Clinton, a placé les nouvelles technologies de l'information au premier rang des principales menaces de la sécurité. Cette dialectique entre crainte et espoir, liés aux N.T.I.C., manifeste leur importance croissante, tout au moins dans les pays –modernes- du G. 7 (G. 8). Cette modernité se caractérise par la gestion du risque, dont la place devient centrale dans la société. L'information apparaît donc comme « un problème touchant la collectivité et appelant une intervention publique », in Gilbert, C., « Le sens caché des risques collectifs », in « la Recherche », n°307, mars 1998.

[31] En 1994, sur proposition de la N.S.A., le gouvernement américain tenta d'imposer un système de cryptographie pour les communications numériques utilisant le système de dépôt des clefs. La solution envisagée reposait sur l'utilisation par le gouvernement d'une puce spéciale, la puce clipper, intégrée dans les équipements de communication, dès leur production, et assurant le cryptage. Le Sénat rejeta cette solution, qui lui parut une forme de contrôle par trop totalitaire, malgré l'absence d'obligation formelle d'utilisation. En introduisant un élément physique sous contrôle étatique dans chaque moyen de communication, l'Etat s'introduisait lui-même physiquement dans la sphère privée.

[32] La cryptographie moderne repose dans sa quasi-totalité sur un modèle commun : afin d'être rendues inexploitables par un tiers, les données sont transformées à l'aide d'un algorithme, qui assure la permanence de la méthode de cryptage et sa portabilité d'un utilisateur à l'autre. L'utilisateur crypte ses données en utilisant un algorithme standard, mais en recourant à une clef qui lui est propre. Pour accéder à ces informations, il est nécessaire de comprendre le mécanisme de chiffrement en analysant l'algorithme, ou de posséder la clef. Cette possession peut être légitime, mais aussi obtenue par des essais successifs pour « casser » le codage. La sécurité d'un tel système repose sur trois points : la puissance de l'algorithme, la taille des clefs en croissance incessante selon l'augmentation des puissances de calcul informatique, et leur gestion.
Il est impératif de résoudre le problème de la transmission des clefs, qui ne peuvent être cryptées, mais qui sont nécessaires au destinataire du message. Cette faille majeure –avant toute transmission sécurisée, il faut transmettre l'élément de sécurisation- a été résolue dès les années soixante-dix par la création de la cryptographie asymétrique, qui utilise un couple de clefs dont une seule est diffusée, ce qui supprime le problème de la sécurité de leur transmission. L'une est la clef privée, qui permet de déchiffrer les messages à l'aide de l'autre, la clef publique. Une fois les données chiffrées avec la clef publique, seul le détenteur de la clef privé peut le décrypter.

matériels de guerre de seconde catégorie, qui correspondent aux «  matériels destinés à porter ou à utiliser au combat des armes à feu ».  Cette réglementation, qui limitait strictement la production et l'utilisation de la cryptographie, était obsolète, tant au regard des nouveaux usages qu'à celui de l'article 233 du Traité de Rome[33], qui n'autorise pas les mesures de protection pour les « produits non destiné à des fins spécifiquement militaires ».

La réforme de 1990, menée dans le cadre de la nouvelle réglementation des télécommunications, constitue une prise en compte des évolutions en matière d'usage. Elle introduit une distinction entre la cryptographie à des fins d'authentification, et celle à des fins de confidentialité. La première est soumise à un régime de déclaration, mais une autorisation du Premier ministre demeure indispensable à la seconde. La législation concernant la cryptographie, qui relève désormais de la réglementation des télécommunications, a été modifiée en 1996. Le texte final précise que cette modification[34] est nécessaire « pour préserver les intérêts de la Défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et transactions sécurisées. » Dès lors, seule la confidentialité demeure soumise à l'autorisation préalable du Service central de sécurité des systèmes d'informations (S.C.S.S.I.). La cryptographie faible, dont les clefs sont inférieures à 40 bits, et l'algorithme connu, est dispensée des formalités d'autorisation.[35] L'usage et la fourniture d'autres moyens assurant la confidentialité par cryptographie restent soumis au principe d'autorisation préalable, de même que leur importation et leur exportation vers des pays extra-européens.

La principale innovation réside dans la mise en place du système des tiers de confiance, ayant reçu l'autorisation du S.C.S.S.I. Ce système constitue l'élément central du dispositif créé par la loi du 26 juillet 1996, et son rôle est de fournir des procédés de cryptographie à ses clients, et de tenir à disposition de l'autorité publique leurs clefs privés. Par cette loi, la puissance publique a voulu libéraliser l'usage de la cryptographie, en gardant comme objectif prioritaire la sécurité collective. Le cœur de la loi ne réside pas dans le contrôle des technologies utilisées, mais dans l'encadrement légal de leur usage. Ce projet fut cependant

[33] 1957.

[34] L'article 17 modifie le deuxième alinéa de la loi du 29 décembre 1990.

[35] Décret d'application n°98-101.

rapidement critiqué, tant d'un point de vue libertaire qu'au vu des risques induits par le système du tiers de confiance. Les problèmes soulevés par cette utilisation de la cryptographie asymétrique contribuent à poser la question de la place et des prérogatives de l'Etat au sein même des réseaux informatiques, et plus particulièrement de l'Internet.

A l'appui des instances nationales, l'Union européenne veut mettre en place une politique juridique et judiciaire de coordination européenne de la lutte contre la cybercriminalité, qui pourrait travailler en accord avec les instances nationales américaines déjà existantes.

### 2.2/ LA COORDINATION INTERNATIONALE DES DEMARCHES INQUISITORIALES ET JUDICIAIRES

Entre l'impératif de dérégulation, qui caractérise les économies avancées, et la nécessité de contrôler les aspects illégaux des télécommunications, se développe une tension telle, qu'elle oblige à maintenir un équilibre entre un degré tolérable d'illégalité et une exploitation créative et rentable de la technologie.

Une collaboration internationale s'est peu à peu mise en place dans le cadre de la lutte mondiale contre la cybercriminalité, lutte qui entraîne des implications importantes pour la détection, l'investigation et la poursuite des criminels. Deux problèmes à caractère international apparaissent liés à cette question. Tout d'abord, la détermination du lieu où le crime a été commis, ce qui décide du système légal applicable à l'acte punissable. Ensuite, la nécessité d'obtenir des preuves selon un système de droit autre, et l'assurance que le contrevenant sera trouvé et traduit en justice. La complexité des accords entre différentes juridictions nationales rejoint alors celle des conventions d'extradition.

Même après avoir décidé quelle juridiction sera appliquée, de nouvelles difficultés apparaissent quant à sa mise en œuvre.[36] De plus, les coûts relatifs à ces poursuites extra-territoriales sont prohibitifs, et la coopération transfrontalière requiert dans ce domaine une

[36] Ainsi dans le cadre d'une juridiction unitaire, comme en Nouvelle-Zélande, déterminer et appliquer la loi nationale appropriée est difficile, mais dans les systèmes fédéraux (Canada, Australie, Etats-Unis…) l'application de lois extra-territoriales est redoutablement complexe.

convergence de valeurs sociales, et de priorités budgétaires, qui n'existe encore que très rarement.[37] D'autres problèmes, liés aux enquêtes, rendent difficiles les recherches et les saisies de matériels en temps voulu. Le volume de documents contenant la preuve, l'utilisation de différentes langues, et le cryptage de l'information ralentissent d'autant les enquêtes, et peuvent les empêcher d'aboutir. La dernière difficulté tient à l'exercice de la souveraineté nationale sur les flux d'informations et les flux financiers. Ainsi, de nombreux problèmes juridictionnels surgissent notamment à propos des transmissions transfrontalières en ligne.[38]

La régulation de la cybercriminalité ne peut pourtant se fonder sur une conception uniquement territoriale de la loi.[39] Depuis le sommet des chefs d'Etat et de gouvernement de juin 1997, les pays les plus industrialisés, soucieux du développement de la criminalité informatique internationale, ont multiplié les déclarations de principe condamnant cette dernière. Néanmoins les différences d'objectifs et de politiques de ces pays ne permettent pas de déboucher sur des résultats concrets et efficaces.

L'Union européenne privilégie les droits de l'homme, alors que les Etats-Unis, paradoxalement au vu de leurs déclarations de principe, protègent avant tout les intérêts étatiques, soit commerciaux et nationaux, et recherchent la collaboration de tout citoyen. Ainsi aux Etats-Unis a été créé un site Web, www.cybercrime.gov, par la Criminal Division's Computer Crime and Intellectual Property Section (C.C.I.P.S.) du U. S. Department of Justice (DOJ). Ce site est consacré à la criminalité informatique, et a pour but d'informer le

---

[37] Certaines pratiques et images qui sont considérées comme acceptables en un endroit sont parfaitement inacceptables ailleurs. Dans certains Etats, la nudité, les œuvres de certains auteurs –Salman Rushdie par exemple-, ou une propagande de mouvements indépendantistes –l'indépendance du Tibet, pour illustrer- seront acceptées sans soucis aucun, ce qui ne favorisera pas la coopération internationale de ces Etats avec ceux qui s'opposent à ces images et discours, les considérant comme des crimes.
Il a, par exemple, fallut trois décennies pour dessiner une modeste assistance mutuelle internationale en matière de lutte contre le trafic de drogues et le blanchiment de l'argent qui en est issu. Il en va de même dans les domaines des copyrights et des accords bancaires internationaux.

[38] Si une lettre de créance en ligne est réalisée en Croatie, et contient des informations frauduleuses à propos d'une entreprise dont les actions sont côtées au Japon, il faut alors s'interroger sur le lieu du crime.

[39] Certaines tentatives nationales officielles, pour bloquer l'accès à des sites, se révèlent infructueuses, en raison de la création de «sites miroirs » dans des juridictions plus permissives. Les tentatives canadiennes de suppression de sites de propagande nazie ont ainsi échoué.

public tout en le renseignant sur les efforts faits par le DOJ pour combattre la criminalité reliée à Internet : en particulier les hackers et ce qui est défini comme crimes contre la propriété intellectuelle.[40]

Des négociations internationales très actives sont menées le plus souvent à l'initiative des Etats-Unis, dans les grandes enceintes internationales (O.C.D.E., Conseil de l'Europe, O.M.P.I., C.N.D.C.I. …), et elles visent à structurer les usages et les comportements sur les réseaux numériques. Il importe que la France et l'Union européenne participe activement à ce débat mondial, faute de quoi elles ne pourront, plus tard, défendre une conception différente de la personne ou du consommateur, ni établir sur les réseaux un « Etat de droit » conforme aux valeurs spécifiquement européennes.

Le Conseil de l'Europe a de son côté élaboré un projet de Convention sur la cybercriminalité, dont le texte évolue rapidement. Les Etats parties à la Convention s'engageraient ainsi à incriminer un certain nombre de comportements. Les infractions visées sont en premier lieu celles concernant la confidentialité des données, leur intégrité et la disponibilité des données et des systèmes informatiques, ainsi que les fraudes informatiques, la pédophilie et les atteintes au droit de la propriété intellectuelle.

C'est conscient de cet enjeu que le Conseil de l'Europe a élaboré en 1989 cette recommandation en matière de criminalité informatique, dans le but d'inciter les Etats membres à adopter des textes répressifs spécifiques, alors que la matière est récente et que l'arsenal pénal existant est souvent déficient ou déjà difficile à appliquer. En 1995, le Conseil de l'Europe a émis une seconde recommandation, relative cette fois aux problèmes de droit de la procédure pénale, liés aux technologies de l'information.

La mise en place d'une coopération des démarches inquisitoriales semble plus encore à l'état de projet que de réalité. En prenant l'exemple d'un pays voisin de la France, cette remarque prend son sens : le gouvernement fédéral belge a fait élaborer et adopter un projet de loi portant sur la criminalité informatique, qui institue une « perquisition virtuelle », concernant quatre catégories d'infraction, définies d'une manière très large.

[40] Cf. annexes, 3. Documents.

Le faux et usage de faux en informatique, qui définit un faux spécifique aux falsifications informatiques, à côté du faux en écriture traditionnel. Cette incrimination vise les personnes qui s'introduisent dans un système informatique, en modifient ou en effacent les données stockées, traitées ou transmises par un système informatique, quel qu'en soit le but, y compris celui de modifier la portée juridique des données. Cette catégorie concerne spécifiquement la fabrication de cartes de crédit falsifiées ou les faux en matière de contrat électronique.

La fraude informatique vise les manipulations de données informatiques dans l'intention de procurer un avantage patrimonial frauduleux. Sous les régimes actuels, les incriminations possibles sont inadaptées dans la plupart des régimes juridiques, et ce type de manipulation échappe aux délits. Deviennent punissables l'utilisation d'une carte de crédit volée pour retirer de l'argent à un guichet automatique, le dépassement illicite du crédit par le biais de sa propre carte de crédit, l'introduction d'instructions informatiques pour modifier le résultat d'opérations en vue d'obtenir un avantage financier, ou le détournement de fichier dans un but de lucre.

Le hacking qui est le fait d'accéder de manière illicite à un système informatique ou de s'y maintenir. De plus, le piratage informatique risque de s'intensifier, en raison du développement des technologies à débits rapides, comme le câble ou l'ADSL (Asymetric Digital Subscriber Line), qui permettent un accès permanent et forfaitaire au Net. L'utilisateur peut alors rester en ligne des heures, ce qui permet au pirate de trouver son adresse IP (Internet Protocol), et d'attaquer son ordinateur. Le texte distingue deux types de hacking, celui commis de l'extérieur et celui commis de l'intérieur, par une personne autorisée mais qui outrepasse ses pouvoirs. Le hacker interne ne devra pas ainsi être animé d'intention frauduleuse ou agir dans le but de nuire, mais cette discrimination curieuse et peu convaincante ne sera sans doute pas acceptée avec le même succès. Par ailleurs, trois comportements spécifiques sont précisés : l'espionnage et le vol de données ; le vol en terme de temps, le blanchiment d'une adresse dans un but d'anonymat ou d'utilisation des ressources, par usage du système informatique ; le fait de causer un dommage par imprudence ; le sabotage vise la manipulation de données effectuées dans le but de nuire, et concerne aussi les actes préparatoires. Néanmoins le commanditaire n'est pas punissable.

Sont de plus punissables l'élaboration et la diffusion frauduleuse des hackertools, outils ou logiciels qui facilitent le hacking.

Enfin, en matière d'instruction criminelle, le projet de loi instaure une « saisie informatique » des données, et prévoit d'instituer, dans le même esprit une forme de perquisition « virtuelle », qui incluent les systèmes informatiques liés. En tenant compte du caractère international des réseaux informatiques, le risque est plus que patent que la perquisition s'exerce sur des données situées en réalité à l'étranger. Dans un tel cas, une coopération transnationale s'avère nécessaire, mais ce projet de loi se contente de préciser qu'alors les données peuvent seulement être copiées. Le juge d'instruction en charge communique alors les données au ministère de la justice, qui informe les autorités compétentes de l'Etat concerné, si celui-ci peut raisonnablement être déterminé. Dès lors, en cas de perquisition « volontaire » de systèmes liés situés à l'étranger, une commission rogatoire internationale devrait en principe être requise, sous peine de porter atteinte à la souveraineté de l'Etat étranger concerné. La mise en pratique d'une telle procédure s'avère en pratique plus que délicate, compliquée d'implications de politique extérieure et d'intérêts commerciaux nationaux divergents, sans compter la lenteur d'un tel système.

Durant quatre ans, le Conseil de l'Europe a cherché à élaborer une convention qui répondrait aux défis de la criminalité informatique, et garantisse la sécurité du réseau mondial et celle de ses utilisateurs. Le comité européen pour les problèmes criminels (C.D.P.C.) avait perçu les risques de l'extension de la criminalité sur le Net, et avait préconisé, suivant en cela l'avis de l'expert mandaté le professeur H. W. K. Kaspersen, la création d'une Convention qui traiterait de la coordination des droits matériels, mais aussi de celle des procédures pénales et des instruments internationaux. En février 1997, le Comité des ministres du Conseil de l'Europe a chargé un nouveau comité d'experts, spécialisés dans l'étude de la criminalité dans le cyberespace, de rédiger un « instrument juridique contraignant », et d'examiner la question des infractions commises, celle de l'obtention de la preuve donc, mais aussi celle des droits pénaux matériels, le recours à des pouvoirs coercitifs, y compris au plan international, et le problème de la compétence vis-à-vis de ces infractions.

En avril 2000, un projet de texte a été déclassifié, une procédure inhabituelle dans l'élaboration des instruments juridiques internationaux, et a été rendu public sur Internet, afin

de recueillir l'avis de tous les professionnels et utilisateurs de ces réseaux. L'Assemblée parlementaire a, en mars 2001, organisé une audition d'experts internationaux, et le Comité des ministres a invité l'Assemblée parlementaire à donner son avis sur ce projet, adopté avec amendements lors de sa session du mois d'avril 2001. Le texte a été approuvé par les délégués des Ministres le 19 septembre 2001, et a été adopté formellement par les Ministres des Affaires étrangères réunis le 08 novembre 2001.

Il a été ouvert à la signature des Etats le 23 novembre 2001, à Budapest, et les ministres ou leurs représentants de 26 Etats membres ont signé le traité : Albanie, Arménie, Autriche, Belgique, Bulgarie, Croatie, Chypre, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Italie, Moldova, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Espagne, Suède, Suisse, « l'ex-République yougoslave de Macédoine », Ukraine et Royaume-Uni. De plus, le Canada, le Japon, l'Afrique du Sud et les Etats-Unis ont participé à son élaboration, et ont également signé la Convention internationale contre la cybercriminalité.

Ce document est le premier traité international à s'intéresser, sous l'angle du droit pénal et des procédures criminelles, aux différents types de comportements délictueux visant les systèmes, les réseaux et les données informatiques, ainsi qu'à d'autres abus de même nature. Le piratage informatique et les dispositifs qui le rendent possible tombent sous le coup du droit pénal des Etats parties à la Convention, tout comme l'interception illégale de données, l'interférence avec des systèmes informatiques, la fraude et la falsification informatiques. Il interdit la pornographie enfantine en ligne, y compris la détention de documents téléchargés de cette nature, ainsi que la reproduction et la diffusion d'œuvres protégées par le droit de la propriété intellectuelle. Il définit les infractions, mais traite aussi des questions relatives à la responsabilité des contrevenants, particuliers ou entreprises, pour lesquels il détermine les normes minimales des peines encourues.

Quant à la répression, les parties auront l'obligation d'habiliter leurs administrations respectives à perquisitionner les systèmes informatiques et à saisir les données, à imposer aux personnes concernées de fournir les données, de les conserver et de les faire conserver. De plus les méthodes d'enquête spécifiques à l'environnement informatique nécessitent la coopération des opérateurs de télécommunication, et des fournisseurs de services Internet, essentiellement pour établir les preuves des méfaits des cybercriminels.

Dans le domaine international, il apparaît que les Etats doivent coopérer pour compléter ces mesures nationales, et le traité enjoint donc les parties à s'accorder une entraide, par exemple en conservant les preuves et en localisant les suspects. Des aspects de la perquisition informatique transfrontalière sont abordés, et les formes traditionnelles d'entraide judiciaire et d'extraction sont applicables dans ce cadre. Un réseau de correspondants en permanence opérationnel est mis en place, de manière à accélérer les enquêtes internationales.

A ces décisions techniques et juridiques de coopération transnationale, des compléments apparaissent indispensables, en matières humaine et financière notamment. Toute solution peut en effet faire appel à une combinaison d'instruments, qui inclut des éléments d'auto-protection (à l'initiative des victimes potentielles), des solutions fondées sur le marché, des initiatives d'auto-régulation (prises par les acteurs soumis à régulation), des mesures coercitives ou régulatrices traditionnelles (du ressort de l'Etat), et la co-production par des tierces parties de formes de surveillance (initiatives privées d'acteurs ou de groupes).

Les Etats et les acteurs privés doivent collaborer dans des missions d'encadrement et de surveillance du réseau, afin d'assurer cette lutte efficace recherchée contre les contenus illicites, et de veiller à la protection effective de la vie privée et des droits des consommateurs et des acteurs des réseaux du cyberespace.

Il s'agit tout d'abord d'encourager les acteurs privés (particuliers et entreprises) à se protéger efficacement, en améliorant leur propre sécurité sur Internet, et en apprenant à en renouveler les moyens régulièrement. Les victimes potentielles doivent apprendre à adopter des comportements prudents, et des mesures positives de protection. Dans de nombreux cas, l'usage de procédures restreignant l'accès aux systèmes informatiques suffit, mais peuvent lui être ajoutées des pratiques managériales rigoureuses : introduction systématique de mots de passe et de procédures de vérification complexes.[41]

[41] Certaines technologies nouvelles améliorent la sécurité des systèmes informatiques : la sécurité bio métrique, les programmes de détection des anomalies.

Face à la mondialisation économique, et dans l'attente d'une régulation internationale pleinement efficace, l'une des solutions peut être une auto-protection alliée à une discipline individuelle de contrôle. Les acteurs privés doivent apprendre à détecter les délits dont ils sont victimes, mais aussi à les dénoncer aux autorités de police. Certains délits ne sont en effet jamais révélés par les entreprises, qui craignent des retombées commerciales pénalisantes, si leurs clients venaient à apprendre le manque de fiabilité de leurs réseaux[42]. Les victimes d'un délit doivent prendre les premières mesures, recourir aux tribunaux quand besoin est, et intenter des actions en dommages, y compris parfois contre les fournisseurs de service. Le risque alors encouru par eux aiderait à augmenter leur vigilance.

De la même manière, le volume du trafic interdisant un contrôle systématique,[43] de nombreux fournisseurs de service exigent désormais comme condition d'accès un engagement de l'utilisateur, qui doit s'interdire toute activité illégale, et respecter un protocole de bonne conduite. Le non respect de cet engagement conduit à une rupture de contrat.

Il s'agit ensuite de développer l'utilisation du Net et de l'informatique comme arme légale pour contrer les délits et crimes informatiques, par le biais de logiciels de recherche adaptés. Le cyberespace peut permettre au contrôle légal de se développer. En effet, cette technologie peut être utilisée pour l'échange d'informations sur la prévention des délits, et peut faciliter le travail d'enquête.[44] Un grand nombre de logiciels commerciaux peuvent être utilisés

---

[42] La criminalité liée aux télécommunications n'est de ce fait pas aisément quantifiable, mais elle peut aussi se révéler trompeuse. Un fait d'apparence anodine peut ainsi conduire à la découverte d'une affaire d'importance. Une illustration classique en est chez Stoll, qui chercha à comprendre une erreur de compte de 0,75 dollar américain dans un système informatique, et découvrit un réseau international d'espionnage.

[43] Des formes de contrôle et de surveillance privées apparaissent : par exemple, le centre Simon Wiesenthal, dont la hotline CyberWatch permet la recherche et la dénonciation de tout matériel raciste ou antisémite. Autre exemple, les Cyber Angels, volontaires recrutés pour patrouiller le cyberspace, recherchant tout matériel illégal. Leurs cibles sont, entre autres, la pornographie enfantine, le développement de virus informatiques, tout ce qui a trait au terrorisme et à la fabrication d'explosifs. En cas d'activités criminelles, l'information recueillie est transmise aux autorités compétentes et aux fournisseurs de service. Tout groupe d'intérêt public encourage les sites web enregistrés sous la mention « sécurisés pour les enfants », ce qui permet aux parents d'utiliser les logiciels adéquats.

[44] Des photographies diffusées sur le Net on conduit à l'arrestation de personnes inscrites sur une liste noire du F.B.I.

pour bloquer l'accès à certains sites. De plus un nouveau marché[45] apparaît : celui des fournisseurs de service spécialisés dans des contenus adaptés à la consommation des familles, et qui garantissent ne rien présenter ayant trait à des contenus contraires aux bonnes mœurs. Un autre marché peut se développer, qui aurait trait au contrôle des pertes en informations causées par une attaque de systèmes de télécommunications. Enfin, le développement d'équipes informatiques de traitement d'urgence (computer emergency response teams C.E.R.T.S.) aide à trouver des solutions aux attaques de système. Ces équipes sont financées par des industries et sont soutenues par des agences de contrôle.[46]

Il s'agit aussi d'étendre les budgets alloués aux recherches judiciaires des crimes informatiques, pour permettre, au moins, l'acquisition à grande échelle du matériel efficace et nécessaire, à la pointe de la technologie. Les technologies de l'information peuvent, en devenant d'usage courant, faciliter les contacts entre les policiers, à l'échelle mondiale. De plus, des budgets supplémentaires peuvent être consacrés à la présence plus fréquente de représentants des services de police à des congrès internationaux sur ces thèmes. Il s'agit enfin de décourager les hackers de travailler pour le compte d'organisations criminelles, et de diffuser des logiciels de décryptage et de « cassage » des codes et mots de passe. Cela nécessite des allocations complémentaires.

Il ne s'agit en fait pas tant de créer des instances supra-étatiques que de permettre et favoriser leur coopération, et de dépasser certaines lenteurs inhérentes aux administrations plus classiques. De la même manière qu'en ce qui concerne la criminalité traditionnelle internationale, la lutte contre la cybercriminalité, qui oblige en démocratie à l'obtention de la preuve est rendue ardue par le ralentissement de la démarche probatoire en raison, non seulement des difficultés d'exécution des commissions rogatoires, et des enquêtes à l'étranger, mais encore par la nécessité de définir l'auteur même de l'acte criminel. En effet, celui-ci est-il l'auteur physique de l'acte, ou bien le commanditaire ? A la cybercriminalité, et d'autant plus qu'elle présente un caractère virtuel, peut s'appliquer le principe de la responsabilité

[45] Sans compter le marché du « data mining » : l'information nominative est vendue et achetée, sous forme de « profils ».

organisationnelle, défini lors des travaux du XVIème Congrès international sur le droit pénal[47] : « dans la mesure où les catégories traditionnelles d'auteur et de complice sont considérées insuffisantes, on devrait envisager une prudente modernisation de ces catégories à partir du principe de la responsabilité organisationnelle ».

Au problème de la régulation du cyberespace peut être appliqué le raisonnement des services de douane américains, qui estiment que puisqu'il n'existe pas de droit applicable spécifiquement au Net, tous les contrôles possibles doivent être effectués, et, de là, le droit évoluera. Ces pratiques offrent un contrepoint aux approches libertaires de certains internautes. Les réseaux de communication SS7 permettront bientôt de fondre les transferts vocaux et de données, qui auront des serveurs de sécurité pour la gestion même des réseaux. Il pourra exister des moyens de contrôle perfectionnés, issus de protocoles de sécurité. Le gouvernement américain, et plus particulièrement le Department of Defence aura en charge peut-être à 40% le développement d'Internet II.

Cet effort technique et financier des autorités américaines est lié à un soucis de contrôle, et la bataille du Communication Licency Act[48], qui voit triompher les libertés individuelles, est contrebalancée par cette nouvelle étape de développement de moyens de contrôle, qui permettront un meilleur travail policier. A l'imitation des Etats-Unis, l'Union européenne, et la France, peuvent sans doute envisager des réformes similaires.

La multiplication des traces informatiques qui touchent aux activités privées des acteurs pousse à s'interroger sur la question du droit à l'oubli, nécessaire à l'équilibre d'une démocratie. Jusqu'à l'informatisation de la société, l'oubli était une contrainte de la mémoire humaine et des archives difficilement exploitables, mais, avec l'informatisation, l'oubli relève désormais plus d'une volonté sociale. Le droit à l'oubli n'est pas nouveau, et ne date pas de la

---

[46] Les forces du marché peuvent également exercer un contrôle du second degré. Les organisations doivent se prémunir contre des actes de piratage informatique, et contre d'éventuelles pertes : il est de l'intérêt des compagnies d'assurance d'exiger de leurs clients la prise de mesures de protection appropriées.

[47] Budapest, 5-11 septembre 1999.

[48] Le Communication Licency Act a été rejeté par la Cour suprême par deux fois, au motif du principe de la protection des libertés individuelles contenu dans le Premier Amendement.

loi du 06 janvier 1978, qui ne le consacre d'ailleurs pas.[49] Une démocratie doit rechercher un juste équilibre entre la vigilance, par la conservation des informations, et l'étouffement, sous les masses de données quotidiennement enregistrées.

## CONCLUSION

Si la cybercriminalité touche les domaines publics et privés, la répression doit en revanche demeurer publique, puisque toute répression juridique touche au cadre régalien de l'Etat. Dans nos sociétés sécularisées, la protection des biens et des personnes contre les infortunes diverses apparaît comme un besoin quasi obsessionnel, le premier des droits. Sous la tutelle d'un Etat non plus providentiel mais protecteur, les Pouvoirs Publics interviennent en dernier ressort, en tant qu'instances de sanction coercitive, mais également de prévention des risques. Les polices, civiles et militaires, se sont en effet imposées historiquement comme les seules agences de régulation et de canalisation, et non seulement de répression.

La gestion de la sécurité n'est pas un processus nouveau pour les Etats, mais Internet lui apporte une dimension supplémentaire d'importance. Le cyberespace est une forme de mort de l'espace public, parce qu'un réseau ne connaît pas la notion d'intérêt général. Cette notion ne présente d'intérêt pour les sociétés démocratiques occidentales qu'au regard d'une question déterminée par le contrat social classique : celle de la confrontation des intérêts privés et publics dans le conflit. Tous ces intérêts ne sont pas compatibles, et doivent être hiérarchisés en fonction du bien commun de la société. Or cette question ne présente aucun intérêt sur le Web où toutes les opinions et tous les besoins sont compatibles, dès lors que les questions techniques d'espace et de flux sont maîtrisées. Les réseaux ne peuvent donc assurer un rôle d'agora, puisque leur but n'est pas la démocratie, mais la communication par groupes spécifiques et renfermés par essence sur un contenu.

[49] Il inspire toute la législation française : l'amnistie, la grâce, la réhabilitation, l'effacement automatique de certaines condamnations après un temps d'épreuve, la prescription. Cet ancien équilibre ne signifie pas que l'impunité soit préférée au civisme.

La transnationalisation, par essence, de la cybercriminalité induit celle du champ juridique pénal, et désormais en ce domaine la norme se fait à un autre plan que celui des Etats. Les ordres juridiques nationaux s'efforcent d'adapter leur législation aux exigences transnationales, car le défi demeure bien celui des systèmes criminels internationaux, informatiques ou non. Le choix de la mise en place de systèmes de contrôle pénal et de répression internationaux n'est donc pas un choix partisan, mais une nécessité.

# ANNEXES

1. Adresses utiles

2. Glossaire

3. Documents

# 1. ADRESSES UTILES

CNIL Commission Nationale Informatique et Libertés
21, rue Saint-Guillaume, 75 007 Paris

DCSSI Direction Centrale de la Sécurité des Systèmes d'Information
18, rue du Docteur-Zamenhof, 92 131 Issy-les-Moulineaux

CLUSIF Club de la Sécurité des Systèmes d'Information Français
18, place des Reflets, 92 975 Paris La Défense Cedex

CIGREF Club Informatique des Grandes Entreprises Françaises
21, rue de Messine, 75 008 Paris

APSAD Assemblée Plénière des Sociétés d'Assurances Dommages
26, boulevard Haussman, 75 311 Paris Cedex 09

APP Agence pour la Protection des Programmes
119, rue de Flandre, 75 019 Paris

AFAI Association Française d'Audit Informatique
88, rue de Courcelles, 75 008 Paris

# 2. GLOSSAIRE

AC : autorité de certification. Entité reconnue et habilitée à gérer des certificats numériques. Permet de mettre en œuvre des systèmes de chiffrement à clés publiques afin de réaliser des services de confidentialité, d'authentification et de non-répudiation.

Adresse de messagerie électronique : identificateur d'un utilisateur d'une application de messagerie électronique.

Adresse logique : identifiant logique d'une ressource indépendant de sa localisation.

Adresse IP : point d'accès au réseau Intenet identifiant un système par rapport à un réseau.

Applet : application développée en langage Java interprétée par une machine virtuelle java et exécutable, en principe, sur n'importe quelle machine.

Application : programme informatique réalisant un service.

Chiffrement asymétrique, à clé publique : système de chiffrement fondé su l'usage d'une bi-clé constituée d'une clé privée secrète et d'une clé publique.

Chiffrement symétrique, à clé privée : système de chiffrement fondé sur l'usage d'une même clé secrète pour chiffrer et déchiffrer une suite d'information.

Contrôle d'accès logique : mécanisme logiciel permettant de contrôler l'accès à des ressources informatiques, fondé sur l'identification, l'authentification et des droits d'accès.

Cookie : variable mémorisée sur une machine cliente web, à la demande du serveur web qu'elle interroge, afin d'en faciliter l'identification.

Cracker : casseur, pirate. Individu qui viole la sécurité d'un système.

Cryptage : chiffrement. Opération de transformation d'un texte clair en un texte chiffré (codé ou cryptogramme) compréhensible seulement par qui dispose du code et de la clé de chiffrement/déchiffrement.

Cyberespace : environnement informatique et de télécommunication constituant un espace géographique virtuel s'appuyant sur des technologies Internet.

DES : Data Encryption Standard : algorithme de chiffrement symétrique adopté en 1977 par le NIST (National Institute of Standards and Technology), Etats-Unis.

DNS : Direction centrale de sécurité des systèmes d'information : www.scssi.gouv.fr, service dépendant du Premier ministre français intervenant entre autres dans le processus d'autorisation d'importation/exportation de produits de chiffrement.

Empreinte numérique : digital fingerprint : permet de s »assurer de l'intégrité des données.

Enveloppe numérique : permet de rendre confidentiel le transfert d'un volume important de données en utilisant conjointement des systèmes de chiffrement symétrique et asymétrique.

Firewall : ordinateur spécialisé dans la réalisation de fonctions de sécurité. Machine placée entre le réseau Internet mondial et un réseau privé afin d'en renforcer le niveau de protection.

Freeware : (graticiel) : désigne les logiciels mis gratuitement à disposition sur le réseau Internet.

Hacker : passioné d'informatique, motivé par la volonté de comprendre et de maîtriser les systèmes informatiques, il es explore afin de découvrir des fonctions non prévue par les concepteurs. Cela peut l'amener à commettre des actes de piratage, devenant alors un cracker (black hat).

HTML : HyperText Mark-up Language : langage de marquage permettant de créer des documents hypertextes manipulés par le web.

HTTP : HypertText Transfer Protocol : protocole de communication assurant le transfert de documents HTML entre clients (navigateurs) et serveurs web.

Internet : selon la définition du J.O. du 16 mars 1999 : « réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destinés à l'échange des messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement, de proche en proche, de messages découpés en paquets indépendants. L'acheminement est fondé sur le protocole IP (Internet Protocol), spécifié par l'Internet Society (ISOC). L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un organisme accrédité. La gestion est décentralisée en réseaux interconnectés. »

Internet Protocol (IP) : protocole contribuant à l'acheminement des données dans un réseau Internet.

ISP : Internet Service Provider, fournisseur d'accès au réseau Internet.

ISO, International Standards Organization : organisme international de normalisation.

ITU, International Telecommunication Union, ex-CCITT, organisme international de normalisation en matière de télécommunication.

Java : langage de programmation proposé par Sun et dont le code peut s'exécuter sur tout type de machine.

Moteur de recherche : logiciel facilitant la recherche d'information sur le web.

Navigateur : logiciel situé dans le poste de travail d'un utilisateur Internet permettant des interactions entre ce dernier et des serveurs web.

Numérique : se dit de la représentation des informations au moyen du langage binaire.

Open source : solution informatique dont le code est librement disponible.

Rfc, request for comments : sigle intervenant dans l'identification de normes de fait de l'environnement Internet, dénommant également le procédé d'établissement de ces normes.

RSA, River, Shamir, Adelman : sigle des noms des inventeurs d'un système de chiffrement à clé publique.

Serveur : machine spécialisée dans la réalisation d'un ou de plusieurs services.

Signature numérique : signature d'un document numérique à l'aide d'un système de chiffrement asymétrique.

Sniffeur : analyseur de protocoles permettant d'espionner le trafic sur un réseau et de récupérer des mots de passe.

Social Engineering : ingénierie sociale : première phase d'une méthode d'attaque consistant à étudier les personnes utilisant ou gérant un système, afin de déterminer qui pourrait être manipulé pour servir les desseins d'un agresseur.

SSL, Secure Sockets Layer : logiciel de protection des flux applicatifs réalisé par l'établissement d'une connexion logique sécurisée entre deux systèmes distants préalablemt à l'échange de données sensibles.

TCP/IP, Transmission Control Protocol/Internet Protocol : protocoles de communication de l'environnement Internet permettant la transmission de données entre entités distantes.

Virus : programme informatique malveillant pouvant entraîner diverses perturbations.

Web : terme utilisé pour désigner le World Wibe Web. Système hypermédia distribué fonctionnant en mode client-serveur et permettant d'accéder à des ressources informatiques réparties à partir de documents hypermédias.

## 3. DOCUMENTS (non inclus dans la version électronique)

- Textes, lois et décrets.

- Services spécialisés.

# BIBLIOGRAPHIE

## I- Ouvrages

BRAIBANT () Donnée personnelles et société de l'information
Rapport au Premier Ministre, transposition en droit français de la directive du n° 95-46.
Paris, Documentation française, 1998

GHERNAOUTI-HÉLIE (s) Internet et sécurité
Paris, P.U.F., Que sais-je ?, 2002

GUISNEL (j) Guerres dans le cyberespace
Paris, La Découverte, 1998

HIMANEN (p) L'éthique hacker et l'esprit de l'ère de l'information
Paris, Exils Editeur, 2001

PANSIER (f-j) et JEZ (e) La criminalité sur Internet
Paris, P.U.F., Que sais-je ?, 2001

PARKER (d.b.) Fighting Computer Crime ; a new Framework for Protecting Information
New-York, éditions Wiley, 2000

ROUACH (d) La veille technologique et l'intelligence économique
Paris, P.U.F., Que sais-je ?, 1999

## II- Articles

« Information et sécurité. Les institutions françaises »

in « Les Cahiers de la Sécurité Intérieure », N°34, 4ème trimestre 1998, pp 109-124
GRABOSKY (p), SMITH (r g) et WRIGHT (p) « Nouvelles technologies, nouveaux délits »
In « Les Cahiers de la Sécurité Intérieure », N°34, 4ème trimestre 1998, pp 13-29

CRETIN (t) « Les puissances criminelles. Une authentique question internationale »
in « RAMSES 2001 », Paris, Dunod, pp 135-154

LETERRE (t) « La démocratie électronique »
in Le Pouvoir, l'Etat, la Politique, Paris, Odile Jacob, Poches, Université de tous les savoirs, volume 9, pp 113-126

OCQUETEAU (f) « Les nouveaux besoins de protection »
in Le Pouvoir, l'Etat, la Politique, Paris, Odile Jacob, Poches, Université de tous les savoirs, volume 9, pp 97-112

PISANI (f) « Penser la cyberguerre »
in « Le Monde diplomatique », août 1999

SOULLIÈRE (n) « Police et innovations technologiques »
in « Les Cahiers de la Sécurité Intérieure », N°34, 4ème trimestre 1998, pp 69-90

## III- Textes de loi

- Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données
- Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance
- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques
- Directive 2000/31/CE du Parlement européen et du Conseil du 08 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du

commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »)

- Code civil : articles 9, 1316, 1316-1, 1316-2, 1316-3, 1316-4, 1317, 1326, 1341, …
- Code de commerce : articles L. 321-3, L. 321-7
- Code pénal : articles 226-15, 227-23, 227-24, 227-28, 323-1, 323-2, 323-3, 323-4, 323-5, 323-6, 323-7
- Code de la consommation : articles L. 121-16, L. 121-18, L. 121-19, L. 121-36
- Code général des impôts : article 289 bis
- Code des postes et des télécommunications : articles L. 32, L. 32-3, L. 32-4, L. 33-1, L. 34-1, L. 34-2
- Code de la propriété intellectuelle : articles L. 341-1, L. 341-2, L. 342-1, L. 342-2, L. 342-3, L. 342-4, L. 342-5, L. 343-1, L. 343-2, L. 343-3, L. 343-4, L. 711-1, L. 712-1
- Loi n° 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises apr la voie des télécommunications
- Loi n° 92-546 du 20 juin 1992 relative au dépôt légal
- Décret n° 81-1142 du 23 décembre 1981 instituant des contraventions de police en cas de violation de certaines dispositions de la loi n° 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décret n°2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

## IV- Sites web de référence

http://www.clusif.asso.fr

http://www.itaudit.org/

http://www.isaca.org/

http://www.sans.org/newlook/home.htm

http://www.assemblee-nat.fr/rapports/r2197.asp

http://www.legalis.net

http://www.infosurance.ch/

http://www.web.mit.edu/security/www/gassp1.html

http://www.oecd.org/dsti/sti/it/secur/index.htm

http://www.bsi.de

http://www.scssi.gouv.fr

http://www.inernet.gouv.fr/francais/index.html

http://www.csrc.nist.gov/

http://www.nsa.gov/

http://www.rsa.com

http://www.securityfocus.com

http://www.cert.org

http://www.fas.org/irp/wwwinfo.html

http://www.cert.org

http://www.radium.ncsc.mil/tpep/library/rainbow

TABLE DES MATIÈRES