

L'identification de l'internaute délinquant

Par : Chemseddine Ethani BARNAT

Enseignant à la Faculté des sciences économiques et

De gestion de Nabeul

Introduction

Dans une intervention dans un colloque organisé par la cour d'appel de Tunis, en collaboration avec l'Institut supérieur de la magistrature, M. Hachemi Kasraoui, substitut du procureur de la République auprès du Tribunal de première instance de Tunis, a défini les crimes informatiques «*comme une atteinte à un droit ou à un intérêt protégé par la loi par le moyen d'un ordinateur, lequel pourrait être un moyen pour commettre le crime ou bien un objet qui subit l'acte criminel à travers une atteinte portée aux systèmes informatiques*»¹.

On utilise souvent des notions voisines, telles que cyber-crime ou cyber-délinquance. Ainsi, il conviendrait plutôt de parler de « cyber-délinquance » plutôt que de « cybercriminalité » qui ne comprendrait que les cas les plus graves de la délinquance virtuelle. Le délinquant étant par définition celui qui est « hors la loi », dans son sens global.

Concrètement la cyber-délinquance comprend deux grandes catégories de menaces potentielles :

- 1) Les menaces non intentionnelles, de type accidentelles (pannes, accidents naturels), ou bien fortuites (erreurs humaines). Elles peuvent résulter d'une négligence de la personne qui se charge de la sécurité.
- 2) Les menaces intentionnelles : passives (ne modifient pas le comportement du système, parfois indétectables), ou bien actives (modification du contenu de l'information).

Cette dernière catégorie correspond parfaitement au profil des pirates ou *hackers*. Ces menaces sont basées sur deux principaux axes : agents techniques² et agents humains³. Les actes classiques perpétrés par les hackers sont essentiellement les suivants :

- Le défacement (altération de sites web) : son but est de transformer la page d'accueil d'un site afin de le ridiculiser
- Espionnage informatique : sous forme d'intrusion à des systèmes informatiques pour dérober des informations utiles.
- Fraudes commerciales : elles touchent essentiellement les cartes bancaires.
- Deni de service : type d'attaque qui entraîne l'indisponibilité d'un service informatique.
- IP *spoofing* : usurpation d'adresse IP (vol d'identité), afin de se faire passer pour quelqu'un d'autre.

¹ Cite par la revue électronique Tunisia today, <http://www.tunisia-today.com/archives/11148>

² Ce sont les techniques utilisées pour réaliser un acte de délinquance, telles que les virus.

³ Ce sont les personnes qui exploitent les techniques d'attaques, pour réaliser leurs objectifs nocifs.

- Le *sniffing* : un espionnage passif en vue de récupérer des informations confidentielles de type log in et mots de passe.

Il est certain que la cybercriminalité ou le crime informatique est aujourd'hui le prix à payer pour l'adoption des toutes nouvelles technologies de communication et d'information. Quelque soit la raison, défier les systèmes informatiques, ou les services de sécurité informatique, ou bien avoir des motivations politiques ou religieuses..., la cyber-délinquance est en train de causer jour après jour des pertes énormes pour l'économie mondiale.

Les chiffres qu'on avance tous les jours sur les pertes dues à la cybercriminalité, nous amène à pousser un cri d'alarme pour faire face à ce phénomène du 21^{ème} siècle. En Tunisie, on a reporté qu'il y a eu en 2005, plus de 500 attaques et vulnérabilités causées, essentiellement, par des virus (vers et chevaux de Troie)⁴, contre 1280 attaque en France en 2003.

Le CSI/FBI (*Computer Security Institute/ Federal Bureau of Investigation*)⁵, dresse chaque année un rapport sur l'état de la sécurité informatique aux Etats-Unis. Ce rapport intégré CSI/FBI est concentré sur un petit panel d'industriels et d'abonnés aux services de l'organisme CSI.

Selon le rapport du CSI/FBI, publié par le CSI en 2005, les personnes sondées déclarent, dans plus de 64 % des cas, avoir été financièrement victimes de fraudes via les NTIC. La moyenne des pertes se situe aux environs de 2,400 \$ par déclaration. Selon le même rapport, 70% des agressions sont jugées sérieuses⁶.

Selon le rapport de 2006, le total des pertes dues aux attaques et fraudes sur Internet sont arrivés en 2006 à 52.494.290\$. Les principales pertes sont comme suit :

- Pertes dues à des contaminations de virus : 15, 691,460\$
- Pertes dues aux accès non autorisés : 10, 610,000\$
- Pertes dues aux fraudes financières : 2, 556,900\$⁷

En 2007, le total des pertes a augmenté pour arriver à 66.930.950\$. Les principales pertes sont comme suit:

- Pertes dues aux fraudes financières : 21, 124,750\$
- Pertes dues à des contaminations de virus : 8, 391,800\$
- Pertes dues aux intrusions : 6, 875,000\$⁸

⁴ Ibid, <http://www.tunisia-today.com/archives/32212>

⁵ Le CSI constitue une des principales organisations mondiales relatives au domaine de la sécurité de l'information. Depuis plus de 30 ans, le CSI aide des milliers de professionnels de sécurité à protéger leurs systèmes d'information, en les sensibilisant *via* des conférences, des publications et divers avantages associés. A ce titre, le CSI édite annuellement un bulletin de sensibilisation lié à la sécurité des systèmes d'information pour des utilisateurs variés : professionnels du monde de la sécurité et autres. Ce bulletin est rédigé en collaboration avec le FBI, service de contre espionnage américain, notamment spécialisé sur la thématique du cyber-crime aux Etats- Unis, *via* son bureau de San Francisco.

⁶ www.gocsi.com

⁷ Eleventh annual report, 2006, CSI, FBI, Computer crime and security survey, by Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, Computer Security Institute, 2006, www.gocsi.com

⁸ 12th annual report, 2007, CSI, FBI, Computer crime and security survey, by Robert Richardson, Computer Security Institute, 2007, www.gocsi.com

Il est à noter que les chiffres recensés se rapportent aux incidents informatiques déclarés. Ces chiffres auraient pu être plus graves si l'on a tenu compte des incidents non déclarés⁹.

Les techniques de fraude sont de plus en plus diversifiées. Du pollupostage (spam), à l'hameçonnage (*phishing*) et le "*pharming*" (la redirection des utilisateurs à leur insu vers des sites Web factices à des fins de fraude), aux intrusions...etc. Autant de techniques qui ne cessent d'embêter aussi bien les utilisateurs de l'Internet que ses gardiens. En 2007, les cinq premières catégories d'infractions¹⁰ commises sur Internet sont les suivantes¹¹ :

- Le vol de services de télécommunication (ou *phreaking*)¹²
- Les communications servant aux activités criminelles classiques¹³
- La violation de la propriété intellectuelle, artistique ou industrielle¹⁴
- La diffusion de contenus immoraux ou dangereux¹⁵.
- Les extorsions et les détournements de fonds¹⁶

En plus des pertes économiques, la cyber-délinquance constitue un défi à la sécurité du cyberspace et au sentiment de confiance qu'on cherche toujours à établir. Le caractère spectaculaire de certaines attaques montre l'audace des cyber-délinquants. Ceux-ci veulent ainsi dire qu'ils sont capables de tout faire et que les mesures prises par les gouvernements sont loin d'être capables d'éradiquer ce fléau¹⁷.

Quoi qu'il en soit, les fraudes informatiques sont aujourd'hui un phénomène marquant du cyberspace dont la communauté internationale essaie de faire face.

⁹ On ne déclare pas toujours les incidents survenus de crainte d'avoir fait une mauvaise publicité pour la société. Certains pensent même que seule 10% des crimes arrivent en justice. Voir à ce propos article publié dans *Tunisia Today*, <http://www.tunisia-today.com/archives/11148>

¹⁰ Les infractions pénales sont classées classiquement en trois catégories : les contraventions, les délits et les crimes. Certaines législations, comme celle de l'Estonie, ont dépassé cette classification trinitaire pour distinguer entre seulement deux catégories d'infractions, à savoir les crimes et les contraventions. Selon l'article 122 du code des procédures pénales, tel que modifié par l'article 3 de la Loi n°89-23 du 27 février 1989, «*Sont qualifiées crimes, aux effets du présent Code, les infractions que les lois punissent de mort, ou de l'emprisonnement pendant plus de cinq ans.*

Sont qualifiées délits, les infractions que les lois punissent de l'emprisonnement d'une durée supérieure à quinze jours et ne dépassant pas cinq années ou d'une amende de plus de soixante dinars. Sont qualifiées contraventions, les infractions que les lois punissent d'une peine ne dépassant pas quinze jours d'emprisonnement ou soixante dinars d'amende ».

¹¹ Voir à ce propos le site *Sécurité Internet*, <http://eservice.free.fr/actualites/0802-categories-cyber-crime-2007.html>

¹² Cela comprend essentiellement : Faire passer des appels sur le compte de tiers (ou via des numéros verts gratuits), revendre des unités de communication sans mandat de l'opérateur et détournement des appels facturés sur une carte téléphonique ou la recharger frauduleusement.

¹³ Cela comprend essentiellement : Le trafic de drogue, les jeux d'argent illégaux, le blanchiment d'argent, la pédophilie et la pornographie infantile, le trafic d'armes.

¹⁴ Cela comprend le piratage de logiciels, de musique, de film, d'e-book, la recopie sans autorisation (sur le Web) de photo, de texte, le développement de la contrefaçon via le spam dans l'industrie du luxe, de la pharmacie, du tabac.

¹⁵ Cela comprend essentiellement, la pornographie adulte et les perversions sexuelles, la propagande des racismes, le mode de fabrication d'engins explosifs, le harcèlement moral, les menaces, les messages intrusifs (par email, mail bombing, par téléphone ...), l'incitation aux agressions physiques.

¹⁶ Les extorsions de fonds sont une forme de cyber-crime lucratif ciblant les personnes morales comme les particuliers.

¹⁷ Parmi les attaques les plus célèbres en Tunisie, la destruction du site animé par des avocats tunisiens pour défendre Saddam Hussein, ou bien les attaques qu'a subi le site de la Société Monétique de Tunisie.

Le législateur tunisien, comme beaucoup d'autres à travers le monde, a mis en place un certain nombre de mesures¹⁸ et de textes incriminant la délinquance informatique. Tel est le cas par exemple des articles 172¹⁹ et 199bis²⁰ du code pénal.

La spécificité de l'Internet est que l'utilisation des réseaux numériques pourrait avoir lieu dans un pays et avoir des retombées dans d'autres pays lointains, chose qui complique la découverte du crime et l'exécution du jugement des tribunaux au cas où son auteur a été identifié. Mais comment peut-on identifier un cyber-délinquant sur Internet ?

L'identification a pour objectif de permettre la poursuite des cyber-délinquants où qu'ils soient. Or, l'identification sur Internet n'est pas une facile affaire. Les difficultés qui existent sont de deux ordres. D'abord, il faut assurer la localisation du délinquant, ensuite assurer son identification.

I- La localisation des internautes délinquants:

La localisation des personnes (et de leurs machines) et la traçabilité des actes commis sur Internet sont deux éléments qui revêtent une importance particulière sur les réseaux numériques. Généralement, on fait recours à l'adresse IP pour la localisation des internautes.

Pour identifier la nationalité de l'internaute dans la chaîne de communication qui lui est transmise par le navigateur, quatre solutions sont envisageables :

1. A partir de l'adresse IP contenue dans les paquets émis par l'internaute et reçus par le fournisseur de d'accès ou le site web.

¹⁸ Plusieurs mesures de luttres contre la délinquance sur internet ont été prises. Ainsi, en Tunisie on a lancé un Cert-TCC : Computer Emergency Response Team - Tunisian Coordination Center (Equipe de réponses aux urgences informatiques Centre de Coordination Tunisien). Le but de ce centre est de fournir une assistance technique en ligne 24/24, collecter et lutter contre les vulnérabilités et les attaques virales... Voir à ce propos : <http://www.ansi.tn/fr/cert-tcc.htm>

¹⁹ Selon l'article 172 du code pénal, « Est puni de l'emprisonnement à vie et d'une amende de mille dinars, tout fonctionnaire public ou assimilé, tout notaire qui dans l'exercice de ses fonctions, commet un faux susceptible de causer un dommage public ou privé et ce, dans les cas suivants:

- En fabriquant, en tout ou en partie, un document ou un acte mensonger, soit en altérant ou en dénaturant un document original par quelque moyen que ce soit, soit en apposant un sceau contrefait ou une signature, soit en attestant faussement l'identité ou l'état des personnes.
- En fabriquant un document mensonger ou en dénaturant sciemment la vérité par quelque moyen que ce soit dans tout support, qu'il soit matériel ou immatériel, d'un document informatique ou électronique, d'un microfilm et d'une microfiche dont l'objet est la preuve d'un droit ou d'un fait générateur d'effets juridiques ».

²⁰ Selon l'article 199 bis du code pénal, tel qu'ajouté par la loi n° 99-89 du 2 août 1999 « Est puni d'un emprisonnement de deux mois à un an et d'une amende de mille dinars ou de l'une de ces deux peines seulement quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données.

La peine est élevée à deux ans d'emprisonnement et l'amende à deux mille dinars lorsqu'il en résulte, même sans intention, une altération ou la destruction du fonctionnement des données existantes dans le système indiqué.

Est puni d'un emprisonnement de trois ans et d'une amende de trois mille dinars, quiconque aura intentionnellement altéré ou détruit le fonctionnement du traitement automatisé.

Est puni d'un emprisonnement de cinq ans et d'une amende de cinq mille dinars, quiconque aura frauduleusement introduit des données dans un système de traitement automatisé de nature à altérer les données que contient le programme ou son mode de traitement ou de transmission.

La peine est portée au double lorsque l'acte susvisé est commis par une personne à l'occasion de l'exercice de son activité professionnelle.

La tentative est punissable.

2. A partir du nom de domaine associé à l'adresse IP
3. A partir de la version linguistique du navigateur utilisée sur le poste de l'utilisateur
4. A partir d'une déclaration de l'utilisateur.

Pour un délinquant les deux dernières possibilités peuvent être, facilement, écartées. Reste donc à savoir si les deux premières possibilités peuvent résoudre le problème de sa localisation.

§1) La localisation à partir de l'adresse IP

A- Le principe de fonctionnement

Chaque ordinateur dispose de sa propre identification sur Internet, ce qui équivaut à une adresse que l'on appelle « adresse IP », composée de quatre nombres, séparés par des points²¹. Le système actuel, dit *v4* est progressivement remplacé par l'IP *v6*, qui permet un plus grand nombre d'adresses²².

L'attribution des adresses IP est placée sous la responsabilité de l'ICANN (*Internet Corporation for Assigned Numbers and Names*) qui la délègue à un organisme chargé de la gestion du serveur souche (*Root Computer*)²³, en l'occurrence la Network Solutions Inc. (*NSI*)²⁴ qui centralise l'ensemble du système d'adressage. Sur la base d'une répartition géographique, l'ICANN distribue les adresses IP aux fournisseurs d'accès, qui sont classés en trois catégories ou classes²⁵.

Si les entreprises et les administrations ont des adresses IP fixes et constantes, les utilisateurs individuels ont, par contre des adresses dynamiques, ou plutôt des sous-adresses fictives, appelées aussi "adresses fantômes". En fait, c'est pour des raisons de gestion des adresses, que le fournisseur d'accès qui en attribue une à la demande. C'est-à-dire, lors de chaque session, selon les plages qui lui sont disponibles, il attribue des adresses IP aux utilisateurs individuels. Autrement dit, à chaque branchement, l'utilisateur a une identification différente.

En principe, il est possible de retracer l'adresse IP de l'utilisateur, et ce pour deux raisons. D'abord, le fournisseur d'accès ne peut attribuer que les adresses IP qui lui sont

²¹ L'adresse IP est numériquement composée d'une suite de quatre nombres, des octets, séparés de points. L'identifiant d'une machine sur le réseau pourra par exemple prendre la forme suivante : 128.121.4.5. Le premier nombre désigne l'adresse du réseau, tandis que le dernier désigne l'adresse de la machine.

²² Deux types d'adresse IP sont actuellement en usage : IP version 4 (IPv4) et IP version 6 (IPv6). IPv4, en service depuis 1983, est la version la plus largement utilisée. Elle utilise des chiffres codés sur 32 bits, ce qui permet la création de 4 milliards d'adresses différentes. Le déploiement du protocole IPv6 a commencé en 1999. Les adresses IPv6 sont codées sur 128 bits, $3,4 \times 10^{38}$ adresses différentes sont donc possibles, soit 340 282 366 920 938 463 463 374 607 431 768 211 456 combinaisons. La notation des adresses IPv6 n'est plus décimale mais hexadécimale, avec 8 groupes de 16 bits séparés par le caractère ":".

²³ Le serveur souche contient les fichiers source permettant de traduire les adresses web en adresses numériques.

²⁴ Jusqu'à il y a peu, la gestion des noms de domaines relevait exclusivement de l'IANA, en vertu d'un mandat *ad hoc* confié par le gouvernement américain. À l'heure actuelle, les noms de domaines sont sous la responsabilité de l'ICANN, l'*Internet Corporation for Assigned Names and Numbers*. L'ICANN, organisme international à but non lucratif, a été créé en 1998, à la suite d'un accord entre Européens et Américains et est en opération depuis 2000. <http://www.renater.fr/Projets/ICANN/>

²⁵ Comme un petit réseau doit adresser moins de machines que les gros réseaux, les adresses IP ont été découpées en plusieurs classes. La classe A permet d'adresser 16.777.214 machines ; La classe B permet d'adresser 65.534 machines ; La classe C permet d'adresser 254 machines.

allouée par l'autorité du Net, sinon celles qu'il a lui-même créées. Ensuite, le fournisseur d'accès dispose des moyens techniques pour savoir quelle personne a été branchée, à quel moment.

En fait, le fournisseur d'accès doit conserver les données servant à identifier les internautes²⁶. En se fondant, sur le numéro de la plage attribué à l'internaute, ainsi que sur les fichiers journaux (logs) de connexion, il est possible de garder une correspondance entre le poste client et son adresse IP. De plus, les informations complémentaires recueillies par le fournisseur d'accès concernant le titulaire de l'adresse IP, comme sa raison sociale, son adresse postale, ses coordonnées téléphoniques, etc., permettent sa localisation géographique.

La localisation géographique ne se fait pas seulement grâce aux rapports entre les fournisseurs d'accès et les postes clients. Mais, plutôt toute opération sur Internet provoque l'enregistrement de l'adresse IP. Par exemple, lors de toute commande de biens ou de services, ou de toute consultation de site, et même de l'envoi d'un e-mail, l'adresse IP est enregistrée, aussi bien chez le fournisseur de service que chez le webmaster du site visité.

Bien que théoriquement la localisation des internautes ne soit pas une tâche très difficile. Il existe quand même, des cas où ça devient plus ou moins compliqué de le faire, surtout lorsqu'il s'agit d'un internaute délinquant.

B- Les difficultés pratiques

En matière pénale, la charge de la preuve incombe à la partie poursuivante, et ce en vertu du principe de la présomption d'innocence. Ainsi, le plaignant doit pouvoir fournir tous les instruments de preuve sur l'infraction, avant qu'elles ne disparaissent²⁷. Or, ce qui est simple théoriquement est plus compliqué en pratique. Cette difficulté spécifique au cyber-crimes, dépend de la personne dont on veut identifier. En fait l'identification d'un internaute ordinaire est relativement plus facile que l'identification d'un internaute délinquant.

La difficulté réside dans le fait que les informations que fournit l'internaute à son fournisseur d'accès sont parfois relativement faibles. Faute de ces informations, certains assimilent la localisation géographique de l'utilisateur à celle de son fournisseur d'accès ou du site qui lui alloue son adresse IP. Or, cette assimilation ne peut faire secours que dans le cas où le fournisseur d'accès est local.

En fait, il existe des situations où il est difficile, de connaître la localisation géographique réelle de l'internaute. C'est ce qui se passe en cas d'usurpation d'identité par exemple. Car, *« contrairement à d'autres protocoles de communication (par exemple : téléphone fixe ou mobile), le protocole IP ne fût pas formellement conçu pour identifier la provenance des données transportées. Cette absence de contrôle facilite la mascarade, ce qui rend notamment l'identification de la source des données peu fiable »*²⁸.

²⁶ Voir article 19 de la loi organique sur la protection des données à caractère personnel, du 24 juillet 2004.

²⁷ Les infractions peuvent être établies par tous moyens de preuve (témoignages, constatations matérielles, indices, présomptions...) et le juge décide d'après son intime conviction".

²⁸ «Yahoo Inc. !, Rapport d'expertise : Etude technique sur les possibilités de filtrage en fonction de la provenance géographique d'internautes ». Disponible sur : www.juriscor.net/txt/jurisfr/cti/tgiparis20000811-rp-def.pdf

Cela peut être réalisé lorsque l'internaute utilise un serveur proxy de connexion²⁹ lors de sa connexion à Internet. Un tel procédé fera en sorte que l'adresse IP de l'internaute sera dissimulée par l'adresse du serveur proxy.

Il existe aussi une autre situation qui brouille la piste de l'investigateur, à savoir le recours à un fournisseur d'accès Internet international. Ainsi, un tunisien peut recourir à un fournisseur d'accès Internet qui fera passer toutes ses communications sur le réseau Internet via une connexion aux Etats Unis et qui pourra lui attribuer une adresse IP américaine. Cet utilisateur sera vu par les sites Internet comme provenant des États-Unis.

En fait, dans ce genre de situations, les postes de travail des utilisateurs résidant sur le territoire tunisien, par exemple, apparaissent sur la toile comme ne résidant pas sur le territoire tunisien. Ces techniques peuvent se justifier pour des raisons de confidentialité et de sécurité des informations transmises. L'affaire *Yahoo!* reflète bien les difficultés liées à la localisation et au « découpage » géographique du cyberspace³⁰.

En fait, dans le cadre de cette affaire, il avait été demandé à un collègue d'experts d'examiner si le moteur de recherche Yahoo!, était en mesure de mettre en œuvre des procédures de filtrage pour interdire l'accès aux internautes opérant à partir du territoire français à des rubriques qui pourraient être jugées illicites par les autorités judiciaires françaises.

Dans son rapport sur la question³¹, François Wallon (l'expert désigné par le juge Gomez), estime que le système de localisation géographique des internautes « *marche très bien dans les cas de fournisseurs d'accès franco-français, mais pas pour AOL, par exemple* »³².

En conclusion le collège d'experts a constaté que seuls 60 à 80% des internautes sont détectables. Les 20 à 40% restants, devraient remplir une déclaration indiquant leurs nationalités. D'où la possibilité de mettre n'importe quel pays et échapper ainsi à toute localisation.

²⁹ Serveur proxy ou serveur mandataire, désigne tout serveur intermédiaire dont la fonction est d'accepter les demandes et de les réexpédier au bon serveur. Le rôle du proxy consiste à se placer entre le navigateur et le site visité de telle sorte que c'est l'adresse IP du proxy qui apparaît et non pas celle du navigateur. En principe lorsque quelqu'un se connecte à un site web, celui-ci doit avoir l'adresse IP du visiteur. Ceci est fait généralement pour des raisons de marketing (ça se vend aux sociétés publicitaires) de plus cela permet d'économiser la bande passante. Exemple de proxy : [Proxomitron](http://www.proxomitron.com), <http://www.anonymizer.com>, <http://megaproxy.com> ou <http://surfola.com>. Pour plus d'informations voir notamment : <http://sebsauvage.net/comprendre/proxy/index.html>

³⁰ Affaire *Yahoo! Inc. C/ la Licra* (Ligue internationale contre le racisme et l'antisémitisme) et l'UEJF (l'Union des étudiants juifs de France), Tribunal de Grande Instance de Paris, arrêt du 22 mai 2000.

³¹ Pour voir le rapport, consulter « *Yahoo Inc.!, Rapport d'expertise : Etude technique sur les possibilités de filtrage en fonction de la provenance géographique d'internautes* ». Disponible sur : www.juriscom.net/txt/jurisfr/cti/tgiparis20000811-rp-def.pdf

³² Dans le même rapport les experts ont fait un examen des moyens techniques disponibles pour contourner ces difficultés. Selon leurs conclusions, le logiciel *Infosplit* et *NetGeo* ne sont pas capables de localiser les internautes utilisant un réseau pour lequel le fournisseur d'accès alloue des adresses IP, ne correspondant pas à la localisation géographique réelle de l'utilisateur. De même, le logiciel *Cyber Locator*, qui repose sur l'exploitation des données géographiques obtenues à partir du système de localisation satellite (GPS), est totalement inadaptés aux besoins de localisation, car rares sont les internautes disposant d'un périphérique GPS couplé avec leur poste de travail. Voir plus de détails sur ce sujet dans le rapport du collège d'experts sur l'adresse suivante : <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001106-rp.htm#texte>

§2) La traçabilité à partir du nom de domaine des sites web

La notion de traçabilité désigne l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'un bien, d'un service ou d'une transaction. La consultation d'une page Web laisse, en principe, des traces tant dans l'ordinateur utilisé que chez le fournisseur de services ou même dans l'ordinateur hôte. De même, les sites Web créés, doivent être déclarés aux autorités dont relèvent les noms de domaine³³.

Il faut distinguer ici entre deux types de noms de domaine. D'abord, ceux qui portent une extension générique ; ensuite, ceux qui portent une extension géographique. Selon l'état actuel des choses, il ne peut y avoir un rapport systématique entre le nom de domaine d'une entreprise et la raison sociale de son activité. De même, il n'y a aucun lien systématique entre le nom de domaine et le lieu où se trouve cette entreprise. Ceci aboutit à la difficulté d'identifier la personne propriétaire du site.

En effet, les sites qui utilisent les extensions génériques (*Top Level Domain*)³⁴ de type (.com), (.org), ou (.net), ne peuvent être localisés à partir de leurs adresses, puisque ce type d'extension n'a pas un rapport avec une activité déterminée, ni avec un pays déterminé. De plus leur attribution n'est pas soumise aux restrictions qu'on impose aux extensions géographiques telles que (.tn).

Ces dernières ne sont pas moins épargnées des problèmes de localisation, puisque le rapport entre l'extension géographique et le pays qui s'y rattache, n'est pas toujours évident. Autrement dit, avoir l'extension (.tn), ne veut pas dire forcément que l'entreprise se trouve en Tunisie, ni que le site est forcément hébergé en Tunisie. Car, tout simplement on peut acheter le nom de domaine et le délocaliser par la suite.

Selon le groupe d'experts désigné lors de l'affaire Yahoo !, « *Il est difficile pour un internaute de savoir si le site qu'il consulte est situé en France ou aux Etats-Unis. Tout au plus, l'internaute peut présumer qu'il a quitté l'espace français si le site consulté n'est pas en langue française, et si l'adresse du site consulté n'est pas dans le domaine de référencement «.fr».* Des cas complexes peuvent apparaître : le nom du site est référencé dans un pays, les machines sont installées dans un second et le site est opéré par une société en provenance d'un troisième »³⁵.

Ainsi, on peut acheter le nom de domaine (.us), juste pour des raisons de marketing, et dissimuler son activité d'escroquerie par exemple. D'ailleurs, la « pauvre » île du pacifique de Tuvalu, dont la population ne dépasse pas les dix mille habitants, s'est vue doter d'une richesse inattendue, grâce à son nom. En fait, cette île vend actuellement cher l'extension (.tv) pour les grandes chaînes de télévision. Ceci montre que le nom de domaine ne veut pas dire forcément que le site est effectivement hébergé dans le pays auquel s'attache cette extension.

Quant aux procédures d'acquisition d'un nom de domaine. Il existe de nombreux « bureaux » d'enregistrement de nom de domaine sur Internet. Ces points de vente et

³³ Les noms de domaines sont une invention de l'américain Johnathan B. Postel, né en 1943 et mort en 1998 au moment où se cristallisait la question de la gouvernance et naissait l'ICANN (*Internet Corporation for Assigned Names and Numbers*). Il avait été jusqu'alors le directeur de l'ICANN.

³⁴ La liste complète des domaines génériques : .aero, .biz, .cat, .com, .coop, .edu, .gov, .info, .jobs, .mobi, .int, .mil, .museum, .name, .net, .org, .pro, et .travel

³⁵ Op.cit., in www.juriscom.net/txt/jurisfr/cti/tgiparis20000811-rp-def.pdf

d'enregistrement des noms de domaine demandent certainement des informations, telles que l'adresse e-mail, et l'adresse de contact ; mais, rien de tout ce qu'on demande n'est réellement vérifiable. Le seul élément qui puisse localiser le site est l'adresse IP du serveur dans lequel est hébergé le site³⁶. Or, ce serveur peut être n'importe où³⁷.

De plus, même si le site est hébergé dans le pays correspondant au nom de domaine, qui empêcherait les responsables du site de le délocaliser pour qu'il soit hébergé dans un autre serveur, dans un autre pays, ou même sur un serveur satellitaire.

Par ailleurs, Internet permet aux entreprises de créer ce qu'on appelle des sites miroirs³⁸. Ces sites peuvent exister dans des endroits différents, afin de faciliter l'accès, en réduisant la distance entre l'utilisateur et le site. Ces sites miroirs, permettent un accès rapide à partir d'un fournisseur d'accès proche. Ainsi, le recours aux adresses visitées par les utilisateurs ne peut pas résoudre le problème de localisation de la source d'une opération, à cause de ces sites miroirs.

Ceci dit, pour localiser une personne agissant à partir d'un site web, la seule possibilité plus ou moins fiable est celle de recourir à l'adresse IP du site pour déduire le pays à partir duquel le délinquant est en train d'agir.

En guise de conclusion, il faut dire que la localisation géographique, constitue certes un problème dans la lutte contre la cyber-délinquance. Mais, les services de sécurité disposent, quand même, de moyens assez développés pour surmonter ce problème, jusqu'à une certaine mesure. L'aide internationale constitue à ce propos un levier important qui permet, en coordonnant les différentes informations, de localiser l'endroit à partir duquel l'infraction a été commise. Toutefois, le problème ne réside pas dans la localisation du cyber-délinquant. Le problème réside plutôt dans l'identification de la personne qui aurait agi derrière le poste d'ordinateur.

§3) La localisation de l'internaute délinquant ne veut pas dire son identification

Parler de la localisation et de l'identification des internautes délinquant, nous impose une question. Est-il possible, à partir d'une connexion Internet de connaître l'identité de celui qui aurait commis une infraction. La réponse à cette question n'est pas toujours évidente.

En fait, pour pouvoir effectuer les poursuites judiciaires contre une personne, il faut tout d'abord que les trois éléments de l'infraction soient présents, à savoir :

- L'élément légal : c'est-à-dire le caractère illégal de l'acte ou du fait en question
- L'élément matériel de l'infraction : constitué par une action ou une omission (en l'occurrence, au minimum un accès non autorisé dans le système, lorsqu'il s'agit d'une action, et d'un manquement à un devoir de surveillance pour le cas d'un responsable du réseau par exemple, lorsqu'il s'agit d'une omission);
- L'élément psychologique ou moral de l'infraction : Celui du caractère frauduleux de l'accès, l'intention, étant caractérisé en matière de fraude informatique par la

³⁶ L'adresse IP sert à faire le lien entre le serveur de l'hébergement et le nom de domaine, par le serveur DNS.

³⁷ Pour faire de l'escroquerie sur internet on peut se servir d'une extension géographique d'un pays pour faire semblant qu'on se trouve dans le même pays que le client par exemple.

³⁸ Sites dont le contenu est identique et localisé dans des endroits différents.

conscience d'avoir pénétré sans droit dans le système par exemple³⁹. De cet élément dérive l'élément de l'imputabilité de l'acte, qui est le fondement même de la culpabilité.

Ainsi, dans la preuve en matière informatique, la difficulté est double. D'une manière générale et sur Internet d'une manière particulière. D'abord, une difficulté au niveau de la matérialité de l'infraction due aux problèmes d'identification ; ensuite au niveau de l'intentionnalité et l'imputabilité de l'infraction⁴⁰.

Concrètement, la difficulté se présente dans le lien qu'il faut établir entre d'une part, les résultats techniques de la recherche de la localisation géographique du poste responsable de l'infraction ; et d'autre part, l'identité de la personne à laquelle le fait incriminé est imputable.

En fait, les serveurs Web enregistrent les informations relatives à la provenance des visites. C'est-à-dire, ils enregistrent les adresses IP des ordinateurs à partir desquels la personne effectue sa connexion, et à travers lesquelles les utilisateurs du réseau sont "identifiés". Or, une telle information ne serait pas d'un grand secours, si on veut identifier la personne physique à qui l'acte ou le fait juridique est imputable. Car, les serveurs n'enregistrent que les caractéristiques techniques de la machine en question (le modèle de la machine, de son microprocesseur, son système d'exploitation), type du navigateur utilisé, adresse IP, le nom de domaine⁴¹. Autrement dit, les serveurs ne donnent pas l'information sur l'identité de l'utilisateur.

Dans le cadre d'un recours préjudiciel déposé le 26 juin 2006 auprès de la Cour de justice des communautés européennes (CJCE). L'avocat général a considéré que : *« le fait que des droits d'auteur aient été enfreints à un moment déterminé sous une adresse IP ne permet pas encore d'affirmer de manière incontestable que c'est le titulaire de la connexion auquel cette adresse aurait été attribuée à ce moment-là qui se serait rendu coupable de ces actes. Au contraire, il est également possible que d'autres personnes aient utilisé sa connexion ou son ordinateur, ce qui peut même avoir été le cas sans qu'il en ait eu connaissance, par exemple, lorsqu'il utilise un réseau local insuffisamment sécurisé pour éviter les liaisons par câble ou lorsque son ordinateur a été «piraté» par des tiers sur l'Internet... [Or], les titulaires de droits d'auteur n'auront aucun intérêt à tenir compte de pareilles circonstances ou à les élucider »*⁴².

Ceci dit, bien que la localisation, soit parfois difficile, elle n'est pas un but en soi. Il faut en plus identifier la personne qui aurait commis la fraude sur Internet. Si les internautes ordinaires ne sont pas en mesure d'échapper facilement aux services de police, les hackers sont, par contre, mieux entraînés pour ce genre d'affaires et prennent généralement plus de précautions.

³⁹ Selon la règle générale pas de crime sans intention, sauf exceptions mentionnées par la loi, et ce surtout en cas d'acte mettant en danger d'autres personnes, ou dans le cas où il y a un manquement à une obligation de prudence.

⁴⁰ En même temps, pour prouver un acte de délinquance sur Internet, il faut absolument tenir compte de deux principes fondamentaux en matière pénale en général : la liberté de la preuve et la présomption d'innocence.

⁴¹ L'utilisateur prendra le plus souvent connaissance de l'adresse sous la forme nominale. Le DNS (*Domain Name System*) relie les adresses numériques aux adresses sous une autre forme que les chiffres, c'est-à-dire aux adresses URL (exemple : www.monadresse.com).

⁴² Voir la Gazette du net, article du 18 juillet 2007, in <http://www.gazettedunet.fr/abonnes/actu,2565.html>

II- Le problème d'identification des cyber-délinquants

Lorsqu'un individu circule dans le monde physique, il est susceptible de faire l'objet de contrôle d'identité tant sur le territoire qu'aux frontières des États. En même temps, tout en circulant, les personnes laissent aussi des traces de leurs passages physiques dans les mémoires d'éventuels témoins, ce qui permet l'identification visuelle dans le cadre des enquêtes judiciaires. Ainsi, l'individu est supposé connaître, même sans en avoir toujours pleinement conscience, le dévoilement de son nom et de son image.

En revanche, plusieurs personnes sont capables de dissimuler leurs identités de telle sorte qu'elles puissent déambuler sur Internet d'une manière quasi-invisible. Ceci peut être fait grâce au développement des techniques d'anonymat. De même que tout passage sur un site et toute expédition de message, peut être enregistrés à l'insu des individus.

§1) L'anonymat: droit et limite à l'identification du cyber-délinquant

A- La notion d'anonymat

Il est difficile de définir le terme « anonymat », car la connotation en est toujours péjorative. Généalogiquement, le mot anonymat remonte aux grecs et plus précisément du mot « *anônumos* », qui signifie sans nom. D'une manière générale, on peut définir l'anonymat comme étant l'état d'une personne dont on ignore le nom ou ne fait pas connaître son nom.

Bien que la présentation de l'identité soit une exigence de la vie en société, certains préfèrent ne pas afficher leur identité et rester à l'écart des interactions sociales. Considéré comme une liberté publique en même temps qu'un droit de la personnalité, le droit à l'anonymat constitue un des aspects de la protection de la vie privée. Selon l'article 1^{er} de la loi organique relative à la protection des données à caractère personnel, « *Toute personne a le droit à la protection des données à caractère personnel relatives à sa vie privée comme étant l'un des droits fondamentaux garantis par la constitution...* »⁴³.

En fait, toute personne doit pouvoir bénéficier de la possibilité d'utiliser les techniques qui assurent la confidentialité, et l'intégrité des données qu'elle transmette sur le réseau. En utilisant les moyens d'anonymat renforcés ou non par des techniques de cryptage autorisées par la loi⁴⁴.

L'anonymat procède par l'effacement ou l'omission des données personnelles. Il s'agit, d'une part, des données relatives à l'identité civile : le nom, le domicile, auxquelles viennent s'ajouter des outils d'identification sous forme d'identifiants codés (numéro de sécurité sociale, numéro d'immatriculation du véhicule, numéro de téléphone, numéro de carte de crédit,

⁴³ Loi organique n° 2004-63 sur la protection des données à caractère personnel, du 27 juillet 2004. Selon l'article 9 de la constitution « L'inviolabilité du domicile, le secret de la correspondance et la protection des données personnelles sont garantis, sauf dans les cas exceptionnels prévus par la loi ». De même, le Conseil de l'Europe a reconnu un certain droit à l'anonymat afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées. Il a reconnu en même temps aux Etats le droit de divulguer les informations relatives à l'identification des internautes, afin de retrouver la trace des responsables des actes délictueux. Voir la déclaration du Conseil de l'Europe sur la liberté de communication sur Internet, du 19 juin 2003, disponible en ligne sur : droit et nouvelles technologies <http://www.droit-technologie.org>

⁴⁴ Voir à ce propos le décret n°2001-2727 du 20 novembre 2001 fixant les conditions et les procédures d'utilisation des moyens ou des services de cryptage à travers les réseaux des télécommunications, ainsi que l'exercice des activités y afférentes. Ainsi que le décret de modification n°2007-1071 du 2 mai 2007.

adresse IP) et, d'autre part, des données relatives à l'identité physique : l'apparence physique, le visage, la voix, les empreintes digitales ou génétiques.

Il est donc, impossible d'interdire l'anonymat, tant qu'on est présumé innocent. Une présomption qui protège le droit de bénéficier du droit à l'anonymat et à la vie privée. C'est ainsi que toute personne est libre de communiquer ce qu'elle lui plaît sans craindre que les pouvoirs publics viennent contrôler ses propos, car cela empiéterait sur sa vie privée. Les internautes ont donc le droit de ne pas s'identifier sur le réseau et ainsi de s'exprimer librement.

Pourtant, ce droit à la protection de la vie privée est en contradiction avec un autre principe de droit aussi essentiel que le premier. Il s'agit du principe de la responsabilité, selon lequel, toute personne doit assumer les conséquences de ses actes. Car, si l'anonymat est une liberté, elle cesse dès lors qu'elle lèse l'intérêt légitime d'un tiers⁴⁵.

Pour pouvoir mettre en œuvre ce principe, il faut qu'on puisse savoir qui a fait quoi et quand. Sur Internet cela se passe impérativement par l'identification des personnes agissant dans le cyberspace. L'anonymat ne peut donc qu'empêcher la poursuite des personnes qui auraient commis un acte contraire à la loi. Car, avec l'anonymat il est impossible d'imputer les actes incriminés à des personnes bien déterminés et faire ainsi leur traçabilité.

B- Les différentes techniques d'anonymat

En plus de la technique de l'usurpation d'adresse IP⁴⁶ qui est plutôt l'une des plus anciennes techniques de piratage, il existe sur Internet plusieurs techniques d'anonymats, notamment, l'anonymat dans le P2P et les mails anonymes.

a. Les réseaux *Peer to Peer*⁴⁷ (P2P) :

Ces réseaux permettent à plusieurs utilisateurs de partager des fichiers de différents types, en les répliquant sur les nœuds. Ils utilisent des logiciels particuliers qui permettent de remplir à la fois la fonction de client et de serveur. D'où l'origine de l'appellation *Peer to Peer* (ou pair-à-pair).

⁴⁵ Beaucoup de civilistes défendent cette idée. Voir à ce propos Jean Carbonnier, *Droit civil, 1/ Les personnes*, Paris, P.U.F., 1996, n°35 (p.65) et Gérard Cornu, *Droit civil, Introduction, Les personnes, Les biens*, Paris, Montchrestien, 7ème éd., 1994, v. n°611, p.231.

⁴⁶ C'est une technique de hacking consistant à utiliser l'adresse IP d'une machine de confiance, afin d'en usurper l'identité. Elle permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on usurpe l'adresse IP. De manière plus précise, cette technique permet la création de paquets IP avec une adresse IP source appartenant à quelqu'un d'autre. Cette technique a beaucoup de limites, puisqu'il est désormais impossible d'en faire sur le trafic TCP.

⁴⁷ Peer to Peer ou P2P, désigne un modèle de réseau informatique dont les éléments (les *nœuds*) ne jouent pas exclusivement les rôles de client ou de serveur mais fonctionnent de deux façons, en étant à la fois clients et serveurs des autres nœuds de ces réseaux, contrairement aux systèmes de type client/serveur, au sens habituel du terme. Le premier réseau P2P est le réseau *Napster* apparu en 1999. Il permettait aux utilisateurs de télécharger des fichiers musicaux MP3. Selon une étude effectuée en 2004 sur le réseau eDonkey2000, montre en terme de nombre de fichiers échangés que le premier média est la musique (à peu près la moitié des fichiers disponibles), ensuite les vidéos (à peu près 15%). Voir Clustering in F. Le Fessant, S. Handurukande, A.-M. Kermarrec & L. Massoulié INRIA-Futurs and LIX, Palaiseau, France, Distributed Programming Laboratory, EPFL, Switzerland et Microsoft Research, Cambridge, UK, *Peer to Peer File Sharing Workloads*. Voir à ce propos : <http://iptps04.cs.ucsd.edu/papers/le-fessant-clustering.pdf>

Les fichiers qui sont mis à la disposition du public sont, en grande partie, en contravention avec les règles de droits d'auteurs⁴⁸. En effet, effectuer une copie d'un morceau musical, exige en principe l'accord de son auteur, ou bien s'il s'agit d'une copie privée, le paiement d'une taxe spéciale. Or, ces réseaux se font exonérés de toutes ces obligations, en violation de toutes les législations et les conventions internationales⁴⁹.

Le contrôle de ces réseaux est extrêmement difficile. Cette difficulté est aujourd'hui encore plus difficile à cause des évolutions techniques de ces réseaux, qui sont passés de la première génération, dite centralisée de *Napster*..., à la deuxième génération, dite semi-centralisée de *KaZaA*, *eMule*...⁵⁰ Et enfin la troisième génération, a vu le jour, grâce au couplage effectué entre ces réseaux et les technologies de cryptage⁵¹. Cette génération est dite décentralisée et baptisée abusivement P3P⁵².

Il s'agit d'un système qui permet une grande confidentialité des échanges entre utilisateurs, ainsi que leur anonymat. Le chiffrement se fait par un système asymétrique (clé privée/ clé publique), rendant très difficile aux autorités de remonter la chaîne. On trouve dans cette catégorie *Share*, *WASTE*, *Freenet*, *GNUnet*, *Mute*, *Grouper*, *TribalWeb*, etc.⁵³. C'est la génération *Peer to Peer* chiffrée et anonyme⁵⁴.

⁴⁸ Certains contenus respectent les droits d'auteur, tel que le site (www.jamendo.com).

⁴⁹ Certes la reproduction des produits culturels hors circuit commercial a toujours existé, mais la différence est qu'avec Internet cette possibilité est devenue à grande échelle.

⁵⁰ Cette génération hybride permet de décentraliser la recherche et la récupération d'objets. Son inconvénient est que sa capacité d'anonymat est limitée, d'autant plus qu'elle peine à rendre des résultats lorsque le nombre d'utilisateurs augmente.

⁵¹ Après l'époque *Napster*, on a connu l'époque *KaZaA*, qui est venu pour combler les lacunes de *Napster*, en permettant le téléchargement d'un même fichier de plusieurs sources, afin d'augmenter la vitesse. *KaZaA* a permis une nouvelle disponibilité dans temps de téléchargement. D'abord les utilisateurs ont eu la possibilité de télécharger alors qu'ils font d'autres choses ; ensuite ils ont eu la possibilité de laisser leurs ordinateurs connectés en permanence. En 2003, le réseau *eDonkey* est apparu en ouvrant d'autres possibilités aux utilisateurs. Ainsi, on a vu la technique de fractionnement des fichiers (à peine le téléchargement est commencé, la partie récupérée est déjà disponible). Malgré le succès des générations anciennes, une nouvelle génération est apparue permettant en premier lieu l'anonymat des utilisateurs (époque *Bit Torrent*). Concrètement les données voyagent d'utilisateur à utilisateur de façon cryptée. Ensuite, une autre variante de réseau est apparue, qui dépend, elle aussi, de la technologie du cryptage. Elle est dotée de systèmes de chiffrement variés, elle garantit à ses utilisateur une confidentialité accrue.

⁵² Dans la fiche technique du logiciel *Freenet*, il est indiqué que « *Freenet est un réseau poste à poste conçu pour permettre la distribution d'information sur Internet de manière efficace sans la peur de la censure. Freenet est complètement décentralisé, ce qui signifie qu'il n'y a aucune personne, ni ordinateur ni organisation qui le contrôle.... Freenet ne peut pas être attaqué comme les systèmes centralisés poste à poste tel que Napster. Freenet utilise le routage intelligent et le moyen de cache. Il apprend les requêtes de routage de manière plus efficace. Il fait automatiquement miroir des données populaires et déplace les données là où la demande est la plus grande* ». Voir à ce propos :

<http://www.01net.com/outils/telecharger/windows/Internet/partage/fiches/9032.html>

⁵³ En France la dernière modification du Code de la Propriété intellectuelle de 2006, interdit le téléchargement de fichiers illégaux sur Internet. Voir la loi n°2006-961 relative aux droits d'auteurs et aux droits voisins dans la société de l'information du 01 août 2006. La loi DADVSI, proposé par le député Alain Suguenot, avait pour but de légaliser le *Peer to Peer* mais sous certaines conditions. En créant une nouvelle taxe optionnelle sur l'abonnement à un FAI pour utiliser un système de licence globale encadrant l'utilisation des réseaux *Peer-to-Peer*.

⁵⁴ Bien qu'il n'existe pas un anonymat complet à partir du fait qu'un ordinateur est connecté à Internet. Mais les auteurs de ce réseau estiment qu'ils réalisent un anonymat maximum, et ce par la décentration du réseau et son chiffrement. Ian Clarke, principal promoteur et porte-parole du logiciel *Freenet* estime que « *Freenet apporte aux fournisseurs et aux utilisateurs de l'information un total anonymat* ». Voir à ce propos, [Transfert.net](http://domain39.altern.com/a910), sur : <http://domain39.altern.com/a910>

b. Les mails anonymes :

Les mails anonymes, est une autre technique d'anonymat, qui permet grâce à une certaine configuration et l'exécution de certaines commande sur l'ordinateur de pouvoir envoyer des mails totalement anonymes et passer par son compte e-mail⁵⁵.

Ceci peut être fait grâce à des services appelés "ré-expéditeurs anonymes" qui acceptent les messages arrivants, mais en ayant préalablement supprimé toutes les informations permettant l'identification de l'expéditeur (à savoir, le champ sur le message contenant l'adresse électronique, l'adresse IP de l'auteur du message), ainsi que les sites visités antérieurement.

c. L'usurpation d'identité et des mots de passe

Que la connexion soit permanente ou non l'identification de la personne sur le réseau commence par sa localisation par son adresse IP, ensuite par son identification par lui-même. Ceci est exigé généralement lors des opérations dans lesquelles l'identité de l'interlocuteur est obligatoire, pour pouvoir passer aux autres étapes. Ceci est le cas par exemple, lors de l'envoi d'un mail, ou surtout dans les opérations financières d'achat ou de vente, ou même pour la simple consultation de son compte bancaire.

L'identification de l'utilisateur, par l'introduction d'un mot de passe ne garantit pas que la personne physique obtenant l'accès à l'ordinateur et, par voie de conséquences, potentiellement, au réseau, soit réellement la personne identifiée. En fait, l'introduction d'un mot de passe valide peut être effectuée par une autre personne que le titulaire légitime dudit mot de passe.

Selon l'état de la technique actuelle, plus de 50% des mots de passe peuvent être craqués en moins de 6 minutes⁵⁶. En fait, il existe sur le réseau des logiciels qui sont capables de faire ce travail en un temps record⁵⁷.

En pratique, il existe plusieurs techniques d'usurpation d'identité, qui permettent la réalisation d'attaques à visage masqué, notamment: le *social engineering* et le *spoofing*, de *cracking*, et le *sniffing*, la possession d'un ordinateur par un virus, le key logger...

• Le social engineering

Ce type d'attaque repose essentiellement sur la faiblesse humaine, plus que sur la technique. A l'origine, cette expression désigne l'art et la manière qu'on utilise pour persuader des individus de se plier à ses désirs.

Dans le contexte plus restreint de l'informatique, cette expression désigne « *les astuces, employées par des hackers, pour obtenir des informations qui leur permettent d'accéder à un système : au lieu d'attaquer frontalement le système avec des algorithmes puissants pour*

⁵⁵ Voir à ce propos : <http://membres.lycos.fr/grosouf/arnakes.htm>

⁵⁶ Nicolas Six, « Trop de mots de passe inefficaces sur le réseau », JDN Solutions, disponible sur : http://www.journaldunet.com/solutions/0205/020527_prob_password.shtml

⁵⁷ Example: "John the ripper". Ibid.

déjouer les protections, on tentera tout simplement de tirer les vers du nez d'un collaborateur en se faisant passer au téléphone pour le service de maintenance ou de dépannage... »⁵⁸.

En pratique, ce procédé a pour objectif de faire révéler aux utilisateurs leur mot de passe (de façon volontaire, voire spontanée) ou toute information de nature à compromettre la sécurité du système informatique.

L'illustration la plus classique consiste, pour la personne malintentionnée, à se faire passer pour un technicien. Dans cette hypothèse, le pirate (ou *hacker*) signale qu'il a besoin du mot de passe de l'utilisateur pour effectuer des travaux de maintenance ou d'administration du système informatique.

- **Le *cracking***

La technique du *cracking* se base sur le principe des essais-erreurs. Concrètement le hacker utilise des logiciels portant des dictionnaires de noms communs et de noms propres afin de tenter de forcer l'accès au système. Ces logiciels sont capables de tester des centaines, voire des milliers de mots à la seconde.

Ces programmes, spécialisés pour "cracker" les mots de passe, doivent leur succès à leur principe d'action. D'abord, il existe des logiciels traditionnels, qui contiennent de plus en plus de mots et offrent des possibilités sans cesse plus performantes, comme la prise en compte de variations sur les mots (minuscules ou majuscules au sein du mot, écriture à l'envers, ajout de chiffres à la fin d'un mot...). Ensuite, il y a d'autres types de logiciels, qui utilisent des techniques plus raffinées. Ces logiciels n'explorent pas chaque combinaison possible. Ils s'appuient sur une bibliothèque de mots de passe courants, ce qui leur permet dans certaines conditions d'en casser plus d'un à la seconde.

- **Le hameçonnage ou le *spoofing***

Le *spoofing* est une technique d'usurpation d'identité électronique. Elle consiste à se faire passer pour quelqu'un d'autre afin d'envoyer un virus ou entraîner quelqu'un à divulguer des informations précieuses.

Le « Brand spoofing », est le type le plus dangereux. Il consiste à usurper l'identité des grandes entreprises. Concrètement, l'internaute pourrait recevoir un faux message de sa banque, lui disant, par exemple, que la banque aurait subi une attaque qui aurait perturbé le fonctionnement du système informatique de la banque. Ce qui nécessiterait l'aide du client afin de rétablir les choses en place. Cette aide consisterait à remplir un formulaire contenant des informations confidentielles (nom prénom, numéro de compte, numéro de carte bancaire, code pin...).

- **Le *sniffing***

Le sniffing est une technique qui utilise « *Sorte de sonde que l'on place sur un réseau pour l'écouter, et en particulier récupérer à la volée des informations sensibles, comme des mot de passe, sans que les utilisateurs ou les administrateurs du réseau ne s'en rendent compte. Le renifleur peut être un équipement matériel ou un logiciel (le premier est bien plus*

⁵⁸ JDN, http://www.journaldunet.com/encyclopedie/definition/627/43/20/social_engineering.shtml

puissant et efficace que le second, encore que, la puissance des machines augmentant sans cesse, l'écart se resserre »⁵⁹.

Certains logiciels spécialisés analysent les paquets d'information transmis et cherchent à reconstituer l'information émise. Bien que cette technique ne marche pas avec les données cryptées transmises, elle peut, par contre être complémentaire avec d'autres techniques qui permettent le décryptage des données.

Mais que dit-on lorsque la société *Sophos*, spécialisée dans la sécurité informatique, dévoile qu'un site russe vend le nécessaire du parfait petit pirate pour 15\$⁶⁰. « *Googlebot* » était déjà connu pour ses nuisances à la confidentialité de certaines données. Mais, pour la première fois, on donne l'exemple d'une suppression de site.

- **Les attaques virales**

Les attaques virales sont parmi les moyens d'espionnage et d'usurpation d'identité les plus efficaces. Parmi les attaques les plus dangereuses, on peut citer les *spyware*⁶¹, le *key logger*⁶², la "*porte dérobée*"⁶³, et surtout les Chevaux de Troie. Ce dernier type est le plus utilisé pour manipuler à distance des ordinateurs et agir sous une autre identité.

Initialement un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte "déguisé" sous une fausse apparence), mais qui, une fois installé exerçait une action nocive totalement différente de sa fonction "officielle".

Actuellement, le terme désigne à peu près tout programme viral qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés), pour remplir une tâche hostile à l'insu de l'utilisateur. Parmi les fonctions de ces virus, l'espionnage de l'ordinateur, l'envoi massif de spam, l'ouverture d'un accès pour un pirate, la prise de contrôle de réseaux entiers pour les faire participer à leurs offensives. On parle alors de machines Zombies, pour désigner les ordinateurs qui échappent au contrôle de leurs propriétaires légitimes.

Et comme il existe des millions qui utilisent les mêmes programmes (essentiellement les programmes Windows), les pirates ont donc, théoriquement des millions de cibles, dès qu'une faille est découverte.

Nombreuses sont les infractions qui ont été commises par des internautes délinquants, en profitant de la technique de cheval de Troie. D'ailleurs, nombreux ceux qui ont prétendu avoir perdu le contrôle de leur poste pour dégager leur responsabilité des actes de délinquance, commis via leur machine. Cette stratégie de défense, appelée « *Trojan defence* », a été employée avec succès à différentes reprises. C'est ainsi qu'un britannique, accusé de la détention de 172 photos pédopornographiques, a été innocenté suite au témoignage d'un

⁵⁹ Dictionnaire en ligne alaide.com : <http://www.alaide.com/dico.php?q=sniffer>

⁶⁰ www.sophos.fr

⁶¹ Le Spyware est un logiciel espion qui collecte des informations à partir d'un ordinateur victime avant de les envoyer à un tiers.

⁶² Le key logger est un spyware spécialisé pour espionner les frappes à clavier, afin de les transmettre à un tiers pour les exploiter. Le key logger peut recueillir les mots de passe, les codes d'accès...

⁶³ Les portes dérobées sont des points d'accès à un système d'exploitation ou un logiciel, laissés délibérément par le concepteur du logiciel pour des raisons de test ou de maintenance. Si un pirate découvre ces portes, il peut les exploiter pour accéder au système.

expert rapportant que l'ordinateur de l'accusé était victime de onze Chevaux de Troie. Ceci a aidé la défense de l'inculpé pour dire que le téléchargement des fichiers était fait sans la connaissance, ni de la permission de l'utilisateur⁶⁴.

Alors qui a fait tout ça ? Nul ne eut répondre à cette question, comme c'est d'ailleurs le cas pour beaucoup d'autres⁶⁵. On dit seulement que « *Computer did it* »⁶⁶. Ce trou noir qui caractérise la cyber-délinquance relève ainsi de grands problèmes juridiques relatifs à l'imputabilité de l'infraction, mais aussi au caractère intentionnel de l'infraction. Des problèmes qui emboitent le pas de la cyber-délinquance.

Car, si on se limite aux apparences, on risque de mettre en accusation des gens qui pourrait être des innocents. En même temps si on cherche en profondeur le vrai responsable de ces infractions, on risque de ne rien trouver. Et puis, s'il se trouve qu'un ordinateur est victime d'une attaque virale, de type, cheval de Troie par exemple, qui pourrait confirmer avec certitude que ce n'est pas le propriétaire de l'ordinateur qui aurait orchestré tout cela pour se soustraire de toute responsabilité ?

Malgré tout ce qu'on réalise comme progrès dans le cadre de la lutte contre les hackers et les techniciens de la cyber-délinquance, ceux-ci trouvent toujours des moyens pour échapper aux yeux des services de sécurité et brouiller la piste des investigateurs. Ce qui donne un de plus en faveur des cyber-délinquants au détriment du droit et de la justice.

Mais il ne faut pas oublier aussi qu'une partie de la responsabilité revient aux fournisseurs d'accès et de services, qui doivent collecter le maximum d'informations sur leurs clients. Une telle contribution permettrait certainement de faire face, au moins, à la petite et moyenne délinquance.

§3) L'identification est aussi un problème de collecte d'information

Sur les réseaux numériques, on peut recenser trois facteurs qui favorisent le développement de la cyber-délinquance, et gênent du même coup l'application du droit pénal :

- L'anonymat des personnes qu'il faut impérativement localiser et identifier pour être en droit d'entamer les poursuites ;
- La fugacité et la volatilité des informations numériques et par conséquent, il est tout à fait possible de les modifier voire même de les supprimer à volonté et dans un très court laps de temps. En même temps les services de police doivent préserver les éléments de preuve et s'appuyer sur des données de connexion afin de caractériser l'infraction ;

⁶⁴ Affaire Regina c/Green (UK), juillet 2003; Affaire Regina c/Karl Schofield (avril 2003)...citées par Marie Barel, *Fraude informatique et preuve: la quadrature du cercle*, p. 8, disponible en ligne sur :

http://actes.sstic.org/SSTIC05/Delits_informatiques_et_preuve/SSTIC05-article-Barel-Delits_informatiques_et_preuve.pdf ; voir aussi dans le même sens, Munir Kotadia, *Expert undermines hacking suspect's defence*, Zdnet, 09 octobre 2003, <http://news.zdnet.co.uk/security/0,1000000189,39117033,00.htm>

⁶⁵ Voir Marie Barel, *Fraude informatique et preuve: la quadrature du cercle*, p. 8, disponible en ligne sur :

http://actes.sstic.org/SSTIC05/Delits_informatiques_et_preuve/SSTIC05-Barel-Delits_informatiques_et_preuve.pdf

⁶⁶ Ibid.

• Le caractère transnational des actes illicites sur les réseaux, ce qui rend plus difficile l'efficacité de leur répression essentiellement fondée sur le principe de territorialité.

Ces contraintes juridiques impliquent que la conservation des données pèse essentiellement sur les opérateurs de télécommunications et sur les fournisseurs de services de l'Internet. Leur collaboration constitue une nécessité *sine qua non* pour établir l'identité des délinquants informatiques et la preuve de leurs délits.

A- L'obligation de collecte et de conservation d'informations

Les personnes qui font un abonnement de connexion à Internet, ou qui éditent des informations sur le web, sont tenues de communiquer à leurs hébergeurs les informations permettant leur propre identification. De même, l'hébergeur est pour sa part tenu par une obligation générale de collecte et de détention des informations sur les personnes responsables des sites qu'il héberge⁶⁷. Faute de quoi, le prestataire d'hébergement pourra voir sa responsabilité civile ou pénale engagée, en se basant sur le principe de la responsabilité en cascade⁶⁸.

C'est ainsi que l'article 19 de la loi organique sur la protection des données à caractère personnelles dispose que celui qui traite des données à caractère personnel, tel est le cas des adresses IP des internautes, est tenu de « *sauvegarder les données par la constitution de copies de réserve sécurisées* »⁶⁹.

⁶⁷ Selon l'article 14 du décret n°97-501 du 14 mars 1997, relatif aux services à valeur ajoutée des télécommunications, « *Tout service à valeur ajoutée des télécommunications doit avoir un directeur responsable du contenu du service fourni aux utilisateurs conformément aux dispositions du code de la presse ci-dessus visé* »⁶⁷.

⁶⁸ Selon l'article 68 du code de la presse « *Sont punissables comme acteurs principaux des peines qui constituent la répression des crimes et délits commis par voie de la presse, dans l'ordre ci-après, à savoir :*

- 1) *Les directeurs de publication ou éditeurs, quelles que soient leurs professions et leurs dénominations*
- 2) *A leur défaut, les auteurs,*
- 3) *A défaut des auteurs les imprimeurs ou les fabricants ;*
- 4) *A défaut des imprimeurs ou des fabricants les vendeurs, les distributeurs ou les afficheurs*». Selon l'article 69 du même code, « *Lorsque les directeurs des publications ou les éditeurs sont en cause, les auteurs seront poursuivis comme complices* ».

De même, selon l'article 9§3 de l'arrêté du ministre des communications du 22 mars 1997, portant approbation du cahier des charges, fixant les conditions particulières à la mise en œuvre et l'exploitation des services à valeur ajoutée de télécommunication de type Internet « *Le directeur désigné par le fournisseur de services conformément à l'article 14 du décret n°97-501 du 14 mars 1997 susvisé, et dont le nom doit être communiqué à l'opérateur public concerné, assume la responsabilité du contenu des pages et des serveurs Web qu'il est appelé à héberger dans ses serveurs conformément aux dispositions du code de la presse sus visé.*

Les clients abonnés des services de type INTERNET, propriétaires des pages et des serveurs hébergés, sont également responsables des infractions aux dispositions de la législation et de la réglementation en vigueur. Le directeur est tenu d'assurer une surveillance constante du contenu des serveurs exploités par le fournisseur de services, pour ne pas laisser perdurer des informations contraires à l'ordre public et aux bonnes mœurs ».

Même en cas de cessation d'activité, « *Le directeur doit conserver, pendant une année à compter de la cessation du service, sous sa responsabilité, sur des supports écrits et magnétiques, une copie du contenu des pages et des serveurs hébergés nécessaire à l'administration de la preuve* ».

⁶⁹ Loi organique n° 2004-63 sur la protection des données à caractère personnel, du 27 juillet 2004. Dans le cadre européen, la convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, dispose dans son article 16, intitulé « *Conservation rapide de données informatiques stockées* » que « *1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.*

De même, l'article 8 de l'arrêté du ministre des communications du 22 mars 1997, portant approbation du cahier des charges, fixant les conditions particulières à la mise en œuvre et l'exploitation des services à valeur ajoutée de télécommunication de type Internet, dispose que : « *Le fournisseur de services s'engage à :*

- *Communiquer à l'opérateur public concerné la liste nominative écrite, dûment signée et actualisée, de tous ses abonnés au début de chaque mois et dans un délai ne dépassant en aucun cas le troisième jour ouvrable du mois suivant celui pour lequel la liste est établie ».*

Le même article ajoute que « *Le fournisseur de services s'engage à :*

- *garder confidentielle toute information relative à la vie privée de ses clients abonnés et n'en faire part que dans les cas prévus par la loi ».*

La conservation de ces données peut servir dans les cas où une poursuite judiciaire est engagée. En fait, il est possible de communiquer ces données, exceptionnellement, aux services publics concernés, et surtout aux services de la police judiciaire⁷⁰, chargés de la poursuite des délinquants, et ce sans avoir besoin du consentement de la personne concernée.

Selon l'article 47 de la loi de 2004 : « *Il est interdit de communiquer des données à caractère personnel aux tiers sans le consentement exprès donné par n'importe quel moyen laissant une trace écrite, de la personne concernée, de ses héritiers ou de son tuteur sauf si ces données sont nécessaires à l'exercice des missions confiées aux autorités publiques dans le cadre de la sécurité publique ou de la défense nationale, ou s'avèrent nécessaires à la mise en œuvre des poursuites pénales ou à l'exécution des missions dont elles sont investies conformément aux lois et règlements en vigueur ».*

Ceci veut dire, que les données de connexion de l'internaute, dont le fournisseur de service ou d'accès dispose, peuvent être communiquées dans le cadre d'une enquête judiciaire sans que cela constitue une violation au droit à la protection des données à caractère personnel.

2- *Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.*

3- *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.*

4- *Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15 ».*

L'article 17 de la même convention, intitulé « Conservation et divulgation rapides de données relatives au trafic » dispose relativement à la mise en œuvre de la convention que « *1- Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:*

a- pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b- pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2- *Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15 ».*

⁷⁰ Selon l'article 9 du Code des procédures pénales « *La police judiciaire est chargée de constater les infractions, d'en rassembler les preuves, d'en rechercher les auteurs et de livrer ces derniers aux tribunaux, tant qu'une information n'est pas ouverte ».*

Mais, est ce que cela peut résoudre le problème dans un réseau qui s'étend sur les quatre coins du monde, avec une diversité de cultures et de politiques, notamment concernant l'organisation de l'activité de fournisseur de service de type Internet.

La difficulté réside essentiellement dans le fait que tous les hébergeurs ne détiennent pas toutes les informations nécessaires à l'identification ou ne vérifient pas que les informations collectées soient suffisantes pour identifier les clients⁷¹. En fait, dans plusieurs pays, on n'exige pas assez d'informations sur l'abonné, ou bien on se limite au strict minimum. D'ailleurs, beaucoup s'opposent à l'idée d'obliger les fournisseurs d'accès à vérifier rigoureusement l'identité de leurs clients, sous peine de transformer ces fournisseurs en auxiliaires de justice⁷².

Par ailleurs, bien que la loi oblige ceux qui font la publication sur Internet de faire connaître au public les noms des responsables⁷³, les informations recueillies ne sont pas forcément précises lorsqu'il s'agit un site web, surtout lorsqu'il est hébergé dans un pays qui ne porte pas assez d'importance à ces éléments.

B- Solutions apportées : des solutions peu efficaces

Afin de faire face au problème d'identification, les services de police judiciaire sont appelés à faire des investigations poussées qui permettraient de suivre les agissements de l'internaute délinquant, à dresser son profil de consommation, à le joindre ultérieurement à son adresse pour des offres promotionnelles adaptées à son profil.

En fait, les fournisseurs d'accès ont, en principe, toutes les informations relatives aux mouvements des internautes à travers leurs adresses IP. Ces éléments d'identification peuvent être couplés à d'autre figurant dans des bases des données et permettre ainsi une identification de la personne physique.

Prenant l'exemple d'un internaute délinquant qui utilise un ordinateur à partir d'un « Publinet », pour acheter un produit quelconque en utilisant une carte bancaire volée. Pour l'identifier, on commence par le localiser. Mais la localisation ne suffit pas puisqu'un grand nombre de personnes peuvent y accéder. De plus, aucun registre d'utilisation, avec l'heure et le nom, n'est tenu par le responsable du « Publinet ». C'est grâce à l'adresse physique de livraison des biens achetés que l'on peut traquer le délinquant.

On peut conclure donc, que la localisation géographique n'est pas suffisante en soi pour identifier l'internaute délinquant, mais elle peut être utile pour des investigations

⁷¹ Lorsque l'hébergeur respecte cette obligation et qu'il communique aux autorités compétentes les informations ainsi collectées, alors sa responsabilité sera dérogée tel que cela a été rappelé par le Tribunal de grande instance de Paris dans un jugement rendu le 22 mai 2002 (Affaire Carpe Diem, L. P /S.A. CARPE DIEM). Voir à ce propos Lionet Thoumyre, « *hyperdossier sur la responsabilité des acteurs de l'Internet en France* », en ligne : <http://www.juriscom.net/pro/visu.php?ID=485>

⁷² Avis de la Commission de la protection de la vie privée n°44/2001 du 12 novembre 2001, (juin 2002) 12 *Ubiquité*, Bruxelles, 103, 108.

⁷³ Selon l'article 16 du code de la presse tel que modifié par la loi organique n°88-89, du 02 août 1988, modifiant et complétant la loi n°75-32, du 28 avril 1975, relative au code de la presse « *Tout périodique doit avoir un directeur. Le directeur doit être de nationalité tunisienne, avoir son domicile réel en Tunisie et jouir de ses droits civils et politiques* ». De même selon l'article 18 de cette loi « *Tout périodique doit faire connaître au public les noms de ceux qui en ont la direction....* ».

profondes par les services de police. Toutefois, si cette technique d'investigation peut être fructueuse pour les actes de fraude par exemple, elle n'est pas forcément de même pour les autres aspects de la délinquance sur Internet, tel que dans les attaques virales, ou intrusions. Car, ce genre de délinquance se fait d'une manière brusque et sans laisser de trace. D'autant plus que dans la plupart du temps ça se fait par usurpation d'identité, en prenant possession de postes victimes. Ce qui fait que l'opération peut passer, par les voies légales et "légitimes".

Conclusion

Il est vrai que les moyens juridiques sont nécessaires pour faire face à la cyber-délinquance. Mais, en réalité les services de la police judiciaire comptent essentiellement sur la technique pour défaire les affaires techniques. Ceci est effectué en faisant peser sur les prestataires de services des obligations juridiques, permettant l'identification des personnes et la collectes de traces, à savoir les données relatives au trafic sur la toile. Sans ces données d'identification, de nombreuses poursuites judiciaires risquent de s'avérer stériles.

Ceci pour ainsi dire que la bataille de l'identification est loin d'être gagnée. Malgré toutes les évolutions technologiques, les hackers ont toujours la main haute. La preuve est que jusqu'aujourd'hui on entend parler des attaques contre les sites les plus sécurisés, sans que l'on puisse savoir d'où elles viennent et par qui.
