Image not found or type unknown

Identification de l'internaute délinquant

publié le **30/09/2016**, vu **3393 fois**, Auteur : Fouad Benseghir

Article traitant des techniques utilisées pour identifier un internaute délinquant et des difficultés de cet identification

Introduction :

Il va sans dire que l'identification des utilisateurs d'internet revêt une importance majeure sur les réseaux numériques.

Cette identification a pour objet de permettre de poursuivre les cybercrimes**1** qui se commettent sur internet en dépit des activités qui s'exercent dans beaucoup de cas sous couvert d'anonymat.

La grande question qui se pose est la suivante : est ce qu'il est techniquement parlant possible d'identifier un internaute délinquant ? Si oui, quelles sont ces techniques et quelles en sont les limites ?

I- Identification : les structures

Après avoir présenté les mécanismes de fonctionnement de l'internet, on présentera les principaux acteurs de ce réseau.

A- Internet : le fonctionnement

L'internet (inter-network) est un ensemble de réseaux informatiques privés et publics qui sont interconnectés entre eux grâce à un protocole de communication commun.

1- Qu'est-ce qu' internet ?

Le réseau internet, parfois appelé ''réseau des réseaux'' est composé d'ordinateurs clients et de d'ordinateurs serveurs.

Les postes clients sont en général utilisés par des personnes privées, tandis que les ordinateurs serveurs demeurent en général l'apanage des entreprises et des administrations.

L'Internet, c'est une histoire de tuyaux interconnectés à travers le monde, dans lesquels coule toute sorte d'informations multimédia**2** qui s'achemine d'ordinateurs à ordinateurs répartis dans toute la planète .

Ces tuyaux sont des lignes téléphoniques, des câbles, des fibres optiques ou des lignes spécialisées qui irriguent d'informations multimédia**3** les différents terminaux personnels.

Concrètement, internet se constitue de millions d'ordinateurs et de réseaux reliés entre eux de façon permanente, pour former un super réseau mondial : le réseau des réseaux.

Précisons que jusqu'alors, on imaginait mal internet sans ordinateurs ; cette idée a été

complètement bouleversée aujourd'hui par l'apparition de nouveaux terminaux : téléphones portables, agendas électroniques…

2- Protocoles de communication

Il va sans dire que tous les ordinateurs du monde parlent un même langage de communication. En effet, Le fonctionnement de l'internet est basé sur un protocole (ensemble des règles nécessaires à la communication entre deux machines) baptisé TCP/IP dont l'un des traits caractéristiques est son système d'adressage IP (pour Internet Protocol).

Un protocole de communication est la norme définissant les règles de communication (interprétation des données) entre les ordinateurs d'un même réseau.

Il s'agit d'un langage numérique standardisé au niveau international et utilisable sur tout réseau relié à l'Internet.

TCP-IP est le langage commun parlé par tous les ordinateurs et serveurs pour communiquer entre eux.

Plus précisément, le protocole TCP-IP**4** permet d'envoyer des paquets d'informations d'un ordinateur vers un autre.

Toutefois, l'utilisation du protocole TCP nécessite l'affectation à chaque périphérique une adresse IP**5**.

En effet, tout réseau de communication, qu'il s'agisse du réseau téléphonique ou du réseau internet, nécessite l'attribution de numéros uniques à l'échelle mondiale**6**.

Sur internet, ce numéro qui identifie une machine particulière au niveau mondial est l'adresse IP.

On appelle adresse IP, le numéro qui identifie tout matériel informatique (serveur, routeur, téléphone IP etc.) connecté au réseau informatique utilisant le protocole internet**7**.

C'est cette adresse qui permet aux ordinateurs connectés à internet d'entrer en communication sur le réseau.

Précisons que pour éviter que deux ordinateurs distincts ne se retrouvent avec une adresse identique, les adresses IP sont distribués par bloc (appelés classes) au niveau mondial par l'ICANN**8**.

Ces classes sont attribuées aux gros fournisseurs d'accès internet qui, à leurs tours, les attribuent à leurs abonnés. Chaque fournisseur d'accès dispose donc d'un certain nombre d'adresse IP à assigner à ses clients.

Par conséquent, un utilisateur internet est identifié, tout au long de sa connexion au réseau, par l'adresse IP qui lui a été attribuée par son fournisseur d'accès à internet.

Dans le cas d'une poursuite judiciaire, elle peut être utilisée pour retrouver l'identité d'un internaute via son fournisseur d'accès.

Le numéro constituant l'adresse IP comporte, dans la version 4 du protocole internet, quatre nombres entiers (on parle de 4 octets) compris entre 0 et 255, séparés par des points comme : 212.134.19.1559.

Toutefois, le développement extrêmement rapide d'internet a conduit à la saturation des adresses

IPv4 disponibles. C’est ce qui explique la transition du système d’adressage IPv4 basé sur 4 octets au système IPv6 basé maintenant sur 16 octets.

Avec le système d’adressage IPv6, qui prend maintenant petit à petit le relais**10**, donne une adresse IP définitive et invariable à chaque objet nomade du réseau.

Cela permet d’augmenter de manière considérable le nombre d’adresses IP possibles (plusieurs milliard de milliards).

La structure de l’adresse IP est donc en train de se modifier et sera notamment portée de 4 octets à 16 octets. Dans ces 16 octets, le protocole IPv6 recommande que 6 de ces 16 octets soient constitués par le numéro de série électronique de la carte réseau Ethernet présente sur l’ordinateur personnel.

Une adresse IP comporte 8 nombres, compris entre 0 et 65 535 (notés en hexadécimal), séparés par des deux-points, comme par exemple 1FFF : 0 : A88 : 85A3 : 0 : 0 : AC1F : 800111.

On comprend alors que l’IPv6 est plus identificatrice que l’IPv4 car à chaque ordinateur une adresse IP unique.

En effet, chaque ordinateur et donc chaque internaute transmettra, le plus souvent à son insu et sans qu’il puisse s’y opposé, un numéro de série unique au monde et stable dans le temps.

Ce numéro est transmis quel que soit le service utilisé sur internet : envoi de courrier électronique, forums de discussion, accès aux moteurs de recherche, réseau sociaux…

On comprend de ce qui précède que le fonctionnement même du réseau internet induit une traçabilité de toute action faite sur le net (consultation d’un site, création de contenu, envoi ou réception de courriels…).

En effet, les protocoles de communication utilisés par internet produisent des traces sur tout comportement sur le net, lesquelles traces sont détenues par les acteurs de l’internet.

B- Internet : les acteurs

Dans le cadre de la communication en ligne, Plusieurs prestataires s’interposent entre l’auteur de l’information circulant sur internet et son destinataire. L’intervention de ces acteurs / prestataires est indispensable pour le fonctionnement de l’internet.

Sur ce chef, on doit distinguer entre les prestataires de services et les services connexes dont les fonctions techniques sont complémentaires.

1- Prestataires de services

Les principaux intervenants dans une opération de communication en ligne sont pour l’essentiel : l’opérateur de communication, le fournisseur d’accès à l’internet et le fournisseur d’hébergement.

- Opérateur de télécommunication

L’opérateur de télécommunication permet à l’utilisateur du service de communication en ligne de se connecter à une infrastructure (réseau téléphonique, réseau câblé, réseau sans fil …) sur lequel est diffusée l’Internet.

Il a donc pour principale mission d’assurer la transmission de l’information entre les utilisateurs d’internet.

- Fournisseur d’accès à l’Internet

Le fournisseur d’accès à l’Internet intervient pour mettre en relation ses abonnés avec les sites internet ou les autres utilisateurs de l’internet.

A cette fin, il fournit, par le biais de contrats d’abonnement, des services de connexion à Internet.

- Fournisseur d’hébergement

Le fournisseur d’hébergement permet de mettre à la disposition des utilisateurs de l’internet un service leur permettant de publier des contenus sur le réseau. Plus précisément, l’hébergement consiste à conserver sur le disque dur du matériel informatique du prestataire des informations et à connecter les sites web à l’internet afin de les rendre accessibles aux internautes.

Autrement dit, il met à la disposition des fournisseurs de contenus les moyens techniques leur permettant de les mettre à la disposition du public sur internet.

Le fournisseur d’hébergement a pour rôle de stocker sur son propre serveur l’ensemble des informations qu’il est conduit à recueillir et qui par la suite, seront consultés par les internautes**12**.

2- Services connexes

En plus des prestataires de services internet, d’autres services sont également nécessaires pour le bon fonctionnement de l’internet : Il s’agit des serveurs Proxy et des serveurs DNS.

- Serveur proxy

Le serveur proxy (cache), souvent hébergé par le fournisseur d’accès à l’internet mais pas exclusivement, stocke les pages les plus souvent demandées par les utilisateurs d’internet.

En effet, les fournisseurs d’accès à internet mettent en place des serveurs relais sur lesquels ils font des copies des serveurs les plus demandés et où ils stockent les services déjà été consultés.

Cette technique permet d’améliorer le temps de connexion aux sites internet : lorsqu’un utilisateur demande un site particulier, s’il se trouve déjà sur le cache, le temps de transfert est diminué (conservées localement elles seront plus rapidement accessibles).

Il s’agit de permettre à l’utilisateur d’Internet d’accéder plus rapidement et sans encombrer les réseaux aux informations disponibles.

Sur le plan technique, l’utilisation de Proxy permet également d’optimiser les échanges en allégeant la consommation de bande passante13 pour les fournisseurs d’accès (souvent facturée au volume des informations échangées).

- Serveur DNS

Le système des Noms de Domaine est un ensemble de règles utilisées par les logiciels pour établir (entre autres choses) la correspondance entre des noms de domaine et des adresses IP.

En fait, il assure la traduction des noms de domaine utilisés par les internautes en numéros IP utilisables par les ordinateurs.

Ainsi, lorsqu'il recevra une demande d'accès par exemple au site www.e-com.com, il traduira la demande en un langage compréhensible par la machine soit par exemple, l'adresse : IP 125.25.36.2.

En fait, si les chiffres conviennent parfaitement aux ordinateurs, il n'en va pas de même pour les humains. C'est pourquoi il a été mis en place un système permettant de faire correspondre l'adresse IP avec une adresse plus facilement mémorisable (les noms de domaine) grâce auquel une séquence alphanumérique plus aisée à mémoriser est attribuée à chaque numéro ou adresse IP.

C'est le Domain Name Server, un serveur qui garde en permanence la table de correspondances, qui se charge, de manière transparente pour l'utilisateur, d'assurer cette conversion.

Ainsi, l'adresse IP 125.21.36.2 s'écrira sous une forme plus aisément assimilable du type : www.e-com.com. Ainsi, lorsqu'il recevra une demande d'accès au site www.e-com.com , il traduira la demande en un langage compréhensible par la machine, soit l'adresse IP (en l'espèce 125.21.36.2) des machines, appelées serveurs de noms de domaine, permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.

Précisons enfin que l'identification des internautes peut faire l'objet de deux utilisations : utilisation dans le cadre du marketing électronique (identification du profil de consommation) et utilisation dans le cadre de poursuites pénales (identification des internautes délinquants).

II- Identification : les techniques

La question qui se pose est la suivante : est-il possible, à partir d'une connexion internet, de connaitre l'identité de celui qui aurait commis une infraction ? En principe, la navigation sur l'internet produit un grand nombre de traces identifiants qui permet de suivre le parcours de toute internaute sur le réseau14. Quelles sont alors les moyens et les techniques qui permettent d'identifier les auteurs des cybercrimes**14** ?

A- Identification de l'adresse IP

On la trouve comment cette fameuse adresse IP ? L'adresse IP, qui constitue le point de départ de toute identification sur internet, se trouve sur le fichier log ou bien on la récupère par des cookies.

1- Fichiers journaux (log files)

L'adresse IP qui sert à l'identification des internautes délinquants se trouve dans le fichier log qui contient d'autres informations tout aussi nécessaires pour cette identification.

Le serveur de l'hébergeur d'un site web conserve dans le fichier log les adresses IP des machines ayant été à l'origine des demandes de connexion.

Le fichier log est un fichier texte créé par un logiciel spécifique installé et enregistré sur le serveur du site web et qui permet d'enregistrer l'historique des communications entre un serveur et des postes clients.

C'est un fichier dans lequel une ligne est écrite à chaque demande de l'internaute (changement de

page, téléchargement d’un fichier, …).

De manière générale, le but d’un fichier log est de garder une trace de ce qui se passe sur Internet afin d’avoir une traçabilité en cas d’actes illégales sur le net.

Par conséquent, l’analyse de ce fichier peut être un moyen très efficace pour identifier les internautes délinquants.

Exemple1 : 130.5.48.74[22/May/2008:12:16:57–0100] «GET/content/index.htm HTTP/1.1 » 200 12433131 : cette ligne Indique une requête satisfaite (code retour =200) de téléchargement (GET) d’un objet de 1243 bits, le 22 mai 2008 à 12h16 avec un décalage de -1heure (-0100) par rapport au temps GMT.

Exemple2 : 130.5.48.74[22/May/2008:12:16:57–0100] «GET/content/news.htm HTTP/1.1 » 200 4504 « /content/index.htm » « Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Sv1) »: Le visiteur venait de la page /content/index.htm avec Internet explorer 6.0 installé sur Windows XP SP2.

2- Fichiers témoins (cookies)

Une autre technique importante d’identification et de pistage des internautes passe par l’utilisation des cookies.

En effet, les cookies sont des petits fichiers textes, sorte de code barre informatique que le serveur d’un site web glisse, le plus souvent sans que l’utilisateur ne le sache, au sein du disque dur de l’internaute visitant le site15.

On comprend donc que les fichiers témoins, à la différence des fichiers journaux conservés sur le serveur du site web, sont stockés sur le disque dur de la machine cliente lors de la première visite sur un site donné16.

Précisons que le fichier témoin porte un nom unique ce qui permettra au serveur qui en est à l’origine de le reconnaitre, et ce, quelle que soit l’adresse IP attribuée à la connexion.

Le fichier témoin agit donc comme un identifiant17. L’objectif étant une identification future de l’internaute lors de ses prochaines visites au site en question. Le recours à la technique des cookies vise bien plusieurs finalités :

L’objectif premier de ce fichier informatique est de faciliter la navigation de l’internaute sur le serveur web. Les cookies peuvent en effet faciliter l’accès de l’internaute au site dont il émane et ainsi lui faire gagner du temps.

Les cookies peuvent également profiler l’internaute et reconstituer son parcours lors de sa navigation. Les informations sur la navigation de l’internaute ne peuvent être lues que par le serveur qui les a créées.

Les données récupérées par les cookies peuvent surtout être utilisées dans le cadre d’enquêtes policières ou plus généralement de procédures judiciaires où elles servent à des besoins d’identification.

En effet, les fichiers témoins permettent d’enregistrer des informations relatives à la navigation d’un internaute : pages consultées, la date et l’heure de consultation...

Précisons enfin que que les cookies permettent d’identifier non pas l’internaute, mais l’ordinateur

utilisé par ce dernier.

B- les étapes de l’identification

Avant de présenter le processus d’identification d’un internaute délinquant, on discutera de la conservation des données électroniques permettant cette identification.

1- Conservation des données de connexion

Les données de connexion parmi lesquelles se trouve l’adresse IP constituent un moyen d’identification de l’internaute délinquant.

Afin de faciliter les enquêtes judicaires par une meilleure « traçabilité » des utilisateurs des réseaux, le législateur a imposé aux intermédiaires techniques la conservation des données numériques d’identification.

Les données de connexion peuvent être divisées en trois catégories : les données de connexion simple, les données de navigation et les données de visite.

Les données de connexion simple sont générées chez le fournisseur d’accès à internet : chaque fois qu’un abonné rentre sur le réseau, celui-ci doit donner le nom de compte et le mot de passe qui lui sont associés.

Ces données rassemblent donc les éléments suivants : identité de l’abonné, heure et début de connexion, l’adresse IP qui a été attribuée à l’abonné durant cette connexion.

Les données navigation sont des données relatives aux sites internet visités ou aux services accédés par le titulaire d’une adresse IP connecté à un moment donnée. Ces données sont également générées par le fournisseur d’accès à internet.

Les données de visite sont générées sur les serveurs des sites internet visités, traçant les adresses IP des tiers qui ont visités ces sites à un moment donné. Il faut alors conserver pendant une durée d’une année18, les données électroniques d’identification suivantes :

- Les informations permettant d’identifier l’utilisateur ;

- Les données relatives aux équipements terminaux de communication utilisés ;

- Les caractéristiques techniques ainsi que la date, l’horaire et la durée de chaque communication ;

- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

- Les données permettant d’identifier le ou les destinataires de la communication ;

On comprend de ce qui précède que l’obligation de conservation qui pèse sur les principaux acteurs de l’internet à comme objet les seules données portant sur l’identification des personnes utilisatrices des services fournis par ces opérateurs et les caractéristiques techniques des communications assurées par ces derniers .

Par conséquent, les données recueillies ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit.

Bref, les données de connexion peuvent être utilisées dans le cadre d’enquêtes policières ou plus généralement de procédures judiciaires ou elles servent à des besoins d’identification.

On comprend donc que la conservation de ces données à pour objectif de permettre l'identification des délinquants et de matérialiser des éléments de preuve des infractions.

2- Processus d'identification

Nous avons compris de ce qui précédé que tout réseau de communication, qu'il s'agisse du réseau téléphonique ou du réseau internet, nécessite l'attribution de numéros uniques à l'échelle mondiale.

Sur internet, ce numéro qui identifie une machine particulière au niveau mondial est l'adresse IP de telle sorte que chaque internaute présent sur internet peut être identifié par ce numéro unique.

Par conséquent, l'identification d'un internaute (d'un ordinateur si on veut être plus précis) auteur d'un acte illicite sur le réseau internet est, à priori, simple.

En effet, l'infrastructure du réseau ainsi que le dispositif technique permettant de le faire fonctionner impose à chaque connexion à l'internet d'être identifiable par une adresse IP.

L'identification de l'internaute délinquant se fait grosso modo en trois étapes successives :

Tout d'abord, il faut trouver l'adresse IP de l'ordinateur utilisé dans la commission de l'infraction, celle-ci permettant de déterminer le fournisseur d'accès ;

Ensuite, il faut se tourner vers ce fournisseur d'accès qui peut seul identifier avec certitude l'ordinateur utilisant la connexion internet en question ;

Enfin, les données de connexion dont dispose les fournisseurs d'accès permettent d'identifier l'internaute délinquant.

Or, la seule adresse IP ne suffit pas pour retrouver la personne physique à qui l'acte est imputable. Il faut d'abord pouvoir localiser l'ordinateur à l'origine de l'infraction sur le net.

Pour ce faire, il faut pouvoir identifier le fournisseur d'accès à internet qui à allouer cette adresse, car accéder à internet c'est obligatoirement disposer d'une adresse IP mise à disposition par un fournisseur d'accès à internet.

Cette adresse IP est enregistrée par les machines du réseau qui identifient de la sorte un titulaire, généralement un fournisseur d'accès, lequel sait lui-même à qui l'adresse IP a été attribuée.

Il est en effet théoriquement possible d'identifier grâce à l'adresse IP le prestataire internet qui la détient, et qui est censé connaitre l'identité de la personne à qui il a attribué cette adresse.

III- Identification : les difficultés

Bien que théoriquement l'identification des internautes ne soit pas une tâche très difficile, il existe des cas où ça devient plus compliqué de le faire, surtout lorsqu'il s'agit d'un internaute délinquant.

En effet, Les cybercriminels peuvent utiliser certains procédés afin d'assurer leur anonymat sur Internet rendant par là très difficile toute identification.

A- Variation de l'adresse l'IP

L’adresse IP servant à identifier un internaute délinquant peut elle-même être difficilement identifiable puisque ce dernier peut la falsifier.

En cette matière, on peut évoquer l’IP dynamique et l’IP spoofing.

1- IP dynamique

Une adresse IP peut être attribuée de manière permanente (Adresse IP statique) à une machine, si celle-ci est reliée à un réseau local lui-même connecté de manière permanente à internet.

Ce premier cas peut être comparé à celui de l’abonné au téléphone qui conserve le même numéro durant toute la durée de son abonnement.

L’adresse IP dynamique est une adresse affectée à tout appareil connecté à l’internet, et qui est différente à chaque connexion.

En effet, Le fournisseur d’accès attribue pour la durée de la connexion à internet un numéro IP unique choisi au hasard au sein de la classe d’adresses qu’il a obtenu directement de l’ICANN.

Lors des sessions ultérieures, le même internaute se verra attribuer par le même fournisseur d’accès un numéro IP différent du précédent.

Cette situation peut être comparée à celle d’une personne ne disposant pas d’un abonnement téléphonique et n’utilisant que des cabines téléphoniques et rarement les mêmes.

Il est dans ce cas très complexe de vérifier qui exactement a fait quoi à partir de ladite adresse.

Cependant, dans tous les cas, le fournisseur d’accès va inscrire pour les besoins d’identification en cas d’actes illicites sur le net, dans un journal de bord l’heure et les coordonnées du client à qui il a donné une adresse IP particulière.

A l’heure actuelle, les adresses IP ne sont pas encore définitivement attribuées à chaque ordinateur.

Toutefois, dans un futur proche, les adresses IP seront fixes et seront en conséquence aussi stables que l’adresse d’un appartement ou d’une maison19.

2- IP spoofing

L’IP spoofing est une technique qui permet d’usurper une adresse IP afin de se faire passer pour une autre personne.

Il est ainsi possible à un technicien averti de falsifier son adresse IP et ainsi d’induire en erreur sur l’identité véritable de la connexion.

Cette technique permet à un pirate d’envoyer à une machine des paquets semblant provenir d’une adresse IP autre que celle de la machine du pirate.

Par ailleurs, l’internaute peut utiliser des logiciels spécifiques permettant de cacher ou falsifier son adresse IP, le rendant de ce fait difficilement identifiable.

D’un autre côté, suite au développement extraordinaire qu’a connu l’internet, une pénurie des adresses IP a caractérisée le monde du net. Il a donc fallu trouver une parade pour faire face à cette situation qui risquerait de contrecarrer ce développement.

La solution technique a consisté à faire correspondre plusieurs ordinateurs à une seule adresse IP. En d’autres termes, plusieurs ordinateurs peuvent surfer en même temps via une unique connexion internet, sans pour autant pouvoir être identifié individuellement.

Concrètement, le principe revient à masquer les adresses IP des stations locales (les ordinateurs d’une faculté, d’une entreprise, cybercafé…) sous une adresse globale, le routeur se chargera de faire coïncider les deux.

Les ordinateurs qui se connectent auront la même adresse IP vu de l’extérieur, les machines ne sont pas visibles ou directement identifiables.

Ainsi les stations locales, qui devraient normalement devoir disposer chacune d’une adresse unique sur internet, se verront attribuer une IP privée non routable (virtuelle), seul le routeur disposera d’une IP routable (réelle) reconnue sur le réseau.

Celui-ci masquera les IP privées pour les remplacer par la sienne. Par conséquent, vu de l’extérieur tout se passe comme si seul le routeur était connecté, le réseau local restant invisible.

On comprend de ce qui précède que le routeur permet de masquer l’ensemble des ordinateurs situés à son amont, ce qui complexifie encore plus le processus d’identification.

On peut donc conclure que compte tenu de l’essor d’internet, il existe potentiellement aujourd’hui une multiplicité d’ordinateurs derrière une même adresse IP, et une multiplicité d’individus derrière un même ordinateur (cybercafés, cercle familial….).

Les caractéristiques de l’adresse IP font qu’il est pratiquement impossible d’identifier l’internaute en tant que visiteur unique en se référant uniquement à cet identifiant certes unique mais facilement falsifiable.

B- Passage par un intermédiaire

Une autre technique qui permet de brouiller la piste d’identification d’un internaute délinquant à partir de son adresse IP est le passage par un intermédiaire.

1- Passage par un Proxy

Le passage par un intermédiaire rend parfaitement anonyme l’adresse IP, puisque seul apparaît l’adresse IP d’un proxy ou d’un routeur. Les internautes délinquants peuvent utilisés des serveurs proxy de manière à prévenir toute identification qui pourrait intervenir grâce aux fichiers Log ou aux cookies.

Lorsque l’internaute délinquant utilise un serveur Proxy de connexion lors de sa connexion à Internet, ce n’est plus son adresse IP qui apparait mais celui du serveur.

La même adresse IP peut être attribuée à plusieurs utilisateurs accédant aux services du web à travers unr.

Le principe des serveurs mandataires consiste donc à remplacer au réseau les ad unique serveuresses IP de leurs clients par les leurs.

L’adresse IP visible sur le réseau et qui servira à la demande de la levée d’anonymat, n’est alors que celle d’un intermédiaire, et non celle de la personne qu’on recherche (le délinquant).

2- Passage par un multi-Proxy

Plus grave encore, l’identification de l’internaute délinquant devient davantage plus complexe et un véritable casse-tête en cas de recours à un chainage de Proxy.

Comme cet intermédiaire a précisément pour vocation ou métier l’anonymat de ses clients, il y a peu de chances de réussir à obtenir facilement qu’il divulgue la vraie adresse IP de son client.

Conclusion :

L’identification sur les réseaux numériques constitue un sujet d’actualité au vue de la multiplication des comportements délictuels sur le net.

Cette identification à de nombreuses conséquences juridiques. En ce sens, l’identification des utilisateurs peut apparaitre comme étant un problème juridique bien spécifique au réseau internet.

Toutefois, l’anonymat dans le cyberespace facilité par plusieurs techniques constitue un obstacle majeur pour l’identification des internautes délinquants.

En effet, plusieurs personnes sont capables de dissimuler leur identité de telle sorte qu’elles puissent déambuler sur internet d’une manière quasi-invisible.

Par conséquent, l’adresse IP qui sert de pratiquement l’unique identifiant permettant d’identifier un internaute délinquant, n’est plus une preuve absolue, mais un simple indice falsifiable.

Malgré toutes les évolutions technologiques, la bataille de l’identification des internautes délinquants est loin d’être gagnée. La preuve est que jusqu’aujourd’hui on entend parler d’actes illicites sur le réseau internet , sans que l’on puisse savoir d’où elles viennent et par qui.

Bibliographie :

Ouvrages :

1- Solange ghérnaouti, « la cybercriminalité : le visible et l’invisible », Collection le savoir suisse, 2009.

2- Florain schaifer, « Protection et anonymat sur internet », Micro application, 2001.

3- Jacques vétois, « technologies et usages de l’anonymat sur internet », éd .l’harmattan, 2012.

4- Abbas Jaber, « les infractions commises sur internet », éd. L’harmattan, 2009.

5- Olivier Iteanu, « l’identité numérique en question », éd. Eyrolles, 2008.

6- Philippe atelion & José dordoigne, « TCP/IP et les protocoles internet », éd. ENI, 2006.

7- Cynthia Chassigneux, « vie privée et commerce électronique », éd. L’harmattan, 2004 .

8- André vaucamps, « Notions de base sur les réseaux », éd. Eni, 2009.

Articles :

1- Chamseddine barnat, « l'identification de l'internaute délinquant », Infojuridique, n° 46-47, Mai 2008.

2- Willy duhen, « FAI face à l'anonymat sur internet : vers de nouvelles résponsabilités », Revue terminal, 2010.

3- Jean-Marc dinant, « le visiteur visité », lex Electronica , Vol. 6, n°2, Hiver 2001.

4- André cunquenaire, « l'identification sur l'internet et les noms de domaine : quand l'unicité suscite la multiplicité », Journal des tribunaux, n°146, février 2001.

6-Jean-sébasyien mariez, « Un premier pas vers la mise en place d'un dispositif pértinent de lutte contre l'usurpation d'identité sur internet », Revue droit de l'immatériel, n°43, novembre 2008.

Références :

1 Plusieurs types d'infractions peuvent se commettre sur le cyberespace : diffusion de contenus illicites, pédopornographie, téléchargement illégal, fishing, piratage informatique, piratage d'œuvres numériques, cyberharcellement…

2 Karine DOUPLITZKY, « guide pratique de l'internet », éd. Odile jacob, 2001, P.9.

3 Information : suite de 0 et 1 traduisant un texte, un son, une image.

4 Transport Control Protocol-Internet Protocol : Il s'agit en fait d'une paire de protocoles, le protocole IP permet l'envoi de paquets d'une adresse IP à une autre, mais ne garantit pas qu'ils arrivent à destination sans erreur ni dans l'ordre d'envoi. Pour aboutir à un envoi sans erreur et dans le respect de la séquence, l'IP est souvent associée au protocole TCP.

5 Philippe ATELIN et José DORDOIGNE, « TCP-IP et les protocoles internet », éd . ENI, 2006, P.131.

6 On peut joindre un ordinateur connecté au réseau (local ou internet) en inscrivant son numéro IP dans la barre d'adresse d'un navigateur.

7 Olivier ITEANU, « l'identité numérique en question », éd. Eyrolles, 2010, P.14.

8 The Internet Corporation for Assigned Names and Numbers.

9 Théoriquement, il peut donc y avoir 256.256.256.256, soit environ quatre milliards d'ordinateurs connectés simultanément au réseau internet.

10 Certains systèmes d'exploitation sont déjà compatibles avec IPv6 et des fournisseurs d'accès délivrent déjà des sous-domaines IPv6.

11 On dispose ainsi d'environ 3,4+1038 adresses, soit plus de 667 millions de milliards par millimètre carré de surface terrestre.

12 Remarquons toutefois que l'utilisateur de la communication en ligne (communément appelé internaute) n'est pas toujours un simple consommateur de l'information diffusée en ligne ; il est

aussi, dans certains cas, diffuseur d’information sur internet (web 2.0 par exemple).

13 La bande passante correspond à la grosseur du tuyau reliant un terminal à internet, c’est d’elle que dépend en partie la vitesse de transfert des données. Elle se mesure en Kilo-bits par seconde, ou en méga-bits par seconde.

14 Claude BOURGEOS, « l’anonymat et les nouvelles technologies de l’information », thèse pour le doctorat, soutenue le 24 septembre 2003 à l’université de Paris V, P.437.

15 Keneth LAUDON, « Management des systèmes d’information », éd. PEF, 2010, P .131.

16 Cynthia CHASSIGNEUX, « Vie privée et commerce électronique », éd. Eyrolles, 2004, P.30.

17 Cynthia CHASSIGNEUX, idem, P.31.

18 La durée de conservation des données d’identification est fixée dans la plupart des législations à un maximum de 1 an à compter du jour de l’enregistrement de ces données.

19 Ce dernier problème devrait trouver sa solution dans le passage au Protocole IPv6. Celui-ci permettant d’affecter des adresses IP uniques à chaque dispositif connecté à internet.

Docteur Fouad BENSEGHIR

Expert en Droit Electronique