Chapitre I:

La vie privée sur internet

I. Introduction

Le développement des technologies numériques de l'informatique et des réseaux, et notamment de l'internet, s'est accompagné de la promesse de retombées sociales et économiques du fait de la facilitation des échanges d'informations. Cependant, l'intégration des réseaux mondiaux dans la vie quotidienne et la poursuite des innovations technologiques multipliant les possibilités de recueil de données à caractère personnel.

L'internet a changé énormément de choses, explique Jean-Claude Kauffmann[1] : **«** *C'est un nouveau monde, un nouvel univers qui s'invente, où tout n'est pas que virtuel et à de multiples implications dans le réel. Internet reformule l'ensemble de la société.* **»**

Cependant avec l'internet, les personnes peuvent laisser derrière elles des « empreintes » électroniques ou des enregistrements des « lieux » qu'elles ont visités, des sujets qu'elles ont consultés, des pensées qu'elles ont formulées, des messages qu'elles ont envoyés et des biens et services qu'elles ont achetés. Cela pose des problèmes de vie privée dans la mesure où toutes ces données à caractère personnel exploitables sur ordinateur, qu'elle aient été générées de façon automatique ou non, sont susceptibles d'être recueillies, mémorisées, détaillées, individualisées, croisées ou exploitées pour divers usages dans des lieux géographiquement dispersés partout dans le monde, éventuellement à l'insu du consommateur ou sans son consentement.

Dans ce chapitre nous présentons une vue générale sur la vie privée pour cela on commence par la définition de certains aspects ayant une relation avec la vie privée, les sources de menaces en termes de vie privée ainsi quelques attaques et enfin les technologies permettant la protection de la vie privée sur internet.

[1] Un sociologue français, spécialiste de la vie quotidienne. Il est admis au Centre national de la recherche scientifique (Centre de recherche sur les liens sociaux, Université Paris Descartes -Sorbonne) en 1977.

II. Définitions

Dans cette partie nous montrons quelques définitions pour bien comprendre l'aspect de la vie privée sur internet, nous commençons par la définition des données à caractère personnelle, leurs traitement, la vie privée dans notre vie quotidienne, la vie privée sur internet, vie privée et la législation pour savoir l'influence de la loi sur la vie privée et en termine par la définition de la surveillance et la sécurité.

II.1. Données à caractère personnel

Les données à caractère personnel sont les informations relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique. **[1]**

II.2. Traitement des données à caractère personnel

Le traitement des données à caractère personnel est une opération ou un ensemble d'opérations portant sur des données. La loi le définit de manière large comme tout travail exercé sur la donnée : collecte, transformation, conservation, transmission, consultation, etc. Mais le texte reste neutre face à la technologie utilisée : traitement par ordinateur, par cartes à puces, serveurs Web… Cette précaution est destinée à se prémunir des avancées technologiques inconnues à ce jour. **[2]**

II.3. Vie privée

Le concept de vie privée est flou. Il recouvre une opinion personnelle et un consensus social variable dans le temps et dans l'espace. Ses limites ne sont pas les mêmes au XIXème qu'aujourd'hui. Ses limites ne sont pas les mêmes dans un petit village ou dans une grande ville. Il se définit en opposition à la vie publique.

La vie privée est l'ensemble des activités d'une personne qui relève de son intimité par opposition à la vie publique. Le droit au respect de la vie privée est proclamé par la loi. **[3]**

II.4. Vie privée sur internet

La vie privée sur Internet est une notion plus importante que celle habituellement admise dans la vie de tous les jours. Il est primordial de bien comprendre que toute information non sécurisée mise en ligne peut être accessible par tout le monde. Cette prise de conscience de l'universalité d'Internet et de sa propension à diffuser rapidement une information importante. **[4]**

Vie privée sur Internet est le désir ou le mandat de vie privé personnels concernant les transactions ou la transmission de données via Internet.

Il s'agit de l'exercice de contrôle sur le type et la quantité d'informations sur une personne et qui peut accéder à ces informations. **[28]**

On peut citer des exemples rassemblant les informations qui composent la vie privée d'un utilisateur :

• Nom, race, origine ethnique, religion, nationalité et niveau d'instruction.

• Adresse électronique[2] et adresse IP[3].

• Taille, âge, poids, dossiers médicaux, groupe sanguin, ADN, empreintes digitales et signature vocale.

• Revenus, achats, habitudes de consommation, renseignements bancaires, données sur vos cartes de crédit/débit, rapports de prêt ou de solvabilité et déclarations de revenus.

• Numéro d'assurance sociale ou autres numéros d'identification. **[5]**

II.5. Vie privée et la législation

La frontière qui sépare la vie privée de la vie publique est variable pour chaque personne, cependant, tout le monde a une vie privée. Ce droit à l'intimité de la vie privée est valable pour tous. Si l'on regarde du côté de la loi, cette notion est clairement prise en compte :

• Convention européenne des Droits de l'Homme et des libertés fondamentales :

[2] Chaîne de caractères permettant de recevoir du courrier électronique dans une boîte aux lettres informatique.
[3] Numéro qui identifie chaque ordinateur connecté à Internet.

Art. 8 *« Toutes personnes à droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »*

• Code civil français :

Art. 9 *« Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé »*

•Guides pour l'utilisation de données personnelles informatisées et leurs transmissions internationales : OCDE [4] en septembre 1980, Assemblée Générale de l'ONU [5], en décembre 1990. **[29]**

• Protection des données à caractère personnel : Convention 108 du Conseil de l'Europe (26/01/81), directives 95/46/EC (libre mouvement) et 2002/58/CE (communications électroniques) (remplaçant la directive 97/66/CE)

• Protection des données nominatives -> à caractère personnel : loi "Informatique et Libertés" du 06/01/78, révisée par loi du 6 août 2004 + loi 94-548 (recherche médicale) http://www.cnil.fr/

La loi permet donc de se protéger, et de faire respecter sa vie privée. Si ceci est assez simple avec des acteurs clairement identifiés, il en va autrement avec Internet. **[30]**

II.6. Surveillance

La loi luxembourgeoise sur la protection des personnes à l'égard du traitement des données à caractère personnel du 2 août 2002 définit la surveillance comme « *toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données à caractère personnel d'une ou de plusieurs personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés.* » **[31]**

[4] Organisation internationale d'études économiques, dont les pays membres - des pays développés pour la plupart - ont en commun un système de gouvernement démocratique et une économie de marché.

[5] Organisation internationale, Ses objectifs sont de faciliter la coopération dans les domaines du droit international, de la sécurité internationale, du développement économique, du progrès social, des droits de l'homme et la réalisation à terme de la paix mondiale.

II.7. Sécurité

La sécurité est l'état d'esprit d'une personne qui se sent tranquille et confiante. C'est le sentiment, bien ou mal fondé, d'être à l'abri de tout danger et risque; il associe calme, confiance, quiétude, sérénité, tranquillité, assurance, sûreté. La sécurité informatique, d'une manière générale consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

• L'intégrité : c'est à dire garantir que les données sont bien celles que l'on croit être.

• La confidentialité : consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

• La disponibilité : permettant de maintenir le bon fonctionnement du système d'information.

• Le non répudiation : permettant de garantir qu'une transaction ne peut être niée.

• L'authentification : consistant à assurer que seules les personnes autorisées aient accès aux ressources. **[31]**

III. Les sources de menaces en termes de vie privée

Aujourd'hui, Internet a un vaste domaine d'application : navigation, messagerie[6], commerce électronique[7],... Ce dernier s'est largement démocratisé depuis quelques temps, ce qui nécessite une évolution permanente des moyens de sécurisation.
Malheureusement, dans cette jungle qu'est Internet, les méthodes de piratage ne cessent d'évolué et des millions de personnes sont soumises à des menaces d'intimité. Les entreprises sont engagées non seulement à regarder ce que vous visitez en ligne, mais d'infiltrer les informations et envoyer des messages publicitaires en fonction de votre historique de navigation. **[32]**
Pour cela nous présentons dans cette partie les sources importantes de menaces : moteurs de recherche, photographies sur internet, les sites de réseautage social, les fournisseurs de services, …

[6] Service qui permet d'envoyer et de recevoir des courriels.
[7] Transactions effectuées par des consommateurs et des commerces par l'entremise d'un réseau, à l'aide d'ordinateurs et de systèmes de télécommunication.

III.1. Photographies sur internet

Aujourd'hui beaucoup de gens ont des appareils photo numériques et affiche leurs photos en ligne. Les personnes représentées sur ces photos pourraient ne pas vouloir les faire apparaître sur l'Internet.

Certaines organisations tentent de répondre à cette préoccupation liée à la confidentialité. Par exemple, la conférence Wikimania [8] 2005 exigeait que les photographes aient l'autorisation préalable de la population dans leurs tableaux. **[4]**

En outre, le droit de la responsabilité traditionnelle ne protège pas les personnes qui sont capturés par une photographie en public parce que ce n'est pas compté comme une invasion de la vie privée, ainsi que des photos d'autres peuvent permettre à d'autres personnes à violer la vie privée d'une personne par trouver des informations qui peuvent être utilisées pour les suivre. **[33]**

III.2. Les moteurs de recherches

Les moteurs de recherche ont la capacité de suivre les recherches d'un utilisateur. Les renseignements personnels peuvent être révélés par des recherches, y compris des articles de recherche utilisés, le temps de la recherche, et plus encore. Les moteurs de recherche ont réclamé une nécessité de conserver ces informations afin de fournir de meilleurs services, la protection contre les pressions de la sécurité, et protéger contre la fraude.

Pour le démontrer il suffit de prendre l'exemple de Google qui peut sans trop de soucis associer votre adresse IP avec l'ensemble de vos recherches, phénomène encore accentué si vous possédez un compte mail chez eux, puisqu'alors il aura accès à des informations plus privées sur vous. **[6]**

Fort de ce constat, certains ont décidé de se distinguer comme des moteurs de recherche que « respectent votre vie privée ». On peut citer Ixquick, qui vous l'annonce d'ailleurs de manière très visible sur sa page d'accueil : Ixquick Protège Votre Vie Privée !

Derrière ces annonces, qu'en est-il vraiment ?

Tout d'abord ixquick n'est pas un moteur de recherche, mais plutôt un méta moteur, c'est à dire qu'il va chercher ses résultats dans les autres moteurs de recherche. De cette façon vous ne donnez votre adresse IP associée à une recherche qu'à un seul moteur de recherche tout en bénéficiant des résultats de l'ensemble d'entre eux. Depuis janvier

[8] Le nom des conférences internationales de Wikimedia Foundation, De périodicité annuelle, elles rassemblent les contributeurs aux projets de la Wikimédia Foundation comme Wikipédia et ses projets frères.

2009 ixquick n'enregistre plus les adresses IP. Il n'utilise les cookies qu'à des fins de conservation de la configuration du moteur de recherche, lesquels sont périmés au bout de 90 jours. Il propose également de multiples services destinés à la protection de la vie privée telle que la navigation en https[9]. **[7], [8]**

III.3. Les sites de réseautage social

Les sites de réseautage social peuvent se révéler un merveilleux moyen d'établir des liens. Ils nous permettent de garder le contact avec nos amis, d'échanger des idées avec des collègues dans nos domaines de travail et de partager de l'information avec des gens dont les passetemps et les intérêts sont semblables aux nôtres. **[9]**

Les renseignements personnels affichés sur ces types de sites finissent souvent par être utilisés de manières inattendues. Les employeurs éventuels, les patrons, les parents, les enseignants, les administrateurs d'université et d'autres catégories de gens utilisent les sites de réseautage social pour se renseigner sur les gens.

Et tout cela surprend ceux qui présument que ce qu'ils affichent est du domaine privé. Des gens ont perdu leur emploi, ont raté des entrevues d'emploi et des possibilités éducatives. On les a suspendus de l'école en raison de messages instantanés, d'« affichages muraux » (sur des sites comme Facebook) et d'autres messages qu'ils croyaient à tort constitués des conversations privées avec des amis.

Voici un titre pour donner une idée du genre de choses qui se produisent :

Un étudiant de première année en génie informatique a fait face à des mesures disciplinaires après que des responsables de l'Université Ryerson de Toronto ont découvert qu'il dirigeait un groupe d'étude sur un site de réseautage social. **[10]**

III.4. Les fournisseurs de services Internet

Le fournisseur de services internet[10] est responsable de la bonne utilisation des données. Les personnes concernées peuvent lui demander quelles sont les données qu'il collecte, traite et conserve, de quelle manière et pour quelle finalité. **[4]**

[9] HyperText Transfer Protocol Secure, est un protocole réseau utilisé pour la navigation sécurisée sur le web**,** il offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web.

[10] Prestataire fournissant divers services professionnels liés à Internet, Ce sont notamment l'hébergement de serveurs Web, la création complète de sites Web, la mise en place d'une boutique électronique, etc.

Le fournisseur de service doit donc respecter les procédures appropriées et les technologies qui garantissent la vie privée des personnes concernées et notamment l'intégrité et la confidentialité des données ainsi que la sécurité du réseau et des services fournis.

Le fournisseur de service ne doit pas :

- Lire, supprimer, modifier les messages envoyés à d'autre.
- Collecter, traiter, conserver des données sur les utilisateurs sans que ce soit nécessaire. Il faut une finalité explicite, déterminée et légitime.
- Conserver les données pour une période plus longue que ce qui est nécessaire pour atteindre le but du traitement.

En évoquant ces règles, il ne faut jamais perdre de vue la question de fond suivante : où se situe exactement dans la chaîne de collecte et de traitement le réel danger pour la vie privée ? **[11]**

III.5. Le commerce électronique

On utilise souvent les services de vente en ligne qui nous permettent de rester chez nous en achetant des marchandises sur l'Internet. Un internaute qui veut acheter quelque chose peut entrer dans le site Web de vente, choisir une ou plusieurs marchandises, et puis de façon quelconque, l'internaute doit faire transférer une somme d'argent à la compte bancaire du marchand. Le marchand va envoyer les marchandises choisis chez l'Internaute. Aujourd'hui, l'utilisation de carte crédit est la façon la plus populaire pour le paiement sur l'Internet.

Parmi les risques sur la vie privée de l'internaute:

- Obtention du numéro sur le poste client

Si un virus ou cheval de Troie installé sur le poste du client pourrait facilement intercepter le numéro de sa carte dès sa saisie par l'utilisateur, et l'envoie à un mal individu.

- Interception du numéro durant sa transmission

L'interception d'un numéro de carte bancaire sur l'Internet est le problème le plus fréquemment évoqué lorsqu'on interroge des internautes à s'adonner aux joies du commerce électronique.

- Obtention sur le serveur du marchand

Il y a des risques qui se situent du côté du marchand. Supposons que maintenant le marchand soit honnête, il stocke le numéro de carte bancaire sur son serveur. Si un individu a réussit à attaquer le serveur du marchand, il peut avoir des milliers de numéros de carte, y compris votre numéro.

- Découverte d'un numéro via un logiciel spécifique

Il existe des logiciels qui permettent de générer des numéros de cartes bancaires syntaxiquement valides. Avec une probabilité très petite, un individu qui utilise ce logiciel peut obtenir un numéro qui est égal à votre numéro. **[12]**

IV. Les attaques de la vie privée

IV.1. Vol d'identité

Le vol d'identité (appelé aussi l'usurpation d'identité) c'est l'utilisation de renseignements personnels volés pour usurper l'identité de quelqu'un en vue de commettre une fraude. Le vol peut être commis dans le but d'accéder à des comptes bancaires réels, d'obtenir des prêts bancaires ou à d'autres fins frauduleuses.
Il est intéressant de noter que les catégories de vol d'identité représentant le plus grand pourcentage de victimisation sont respectivement l'utilisation de carte de débit ou crédit avec 3% et les informations personnelles compromises sans fraude avec 2,5%. **[13]**

L'usurpation d'identité débute toujours par la collecte de renseignements personnels sur l'individu fraudé. Les renseignements personnels peuvent être le nom, le numéro de téléphone, la date de naissance, l'adresse, le numéro d'assurance sociale ou toute autre information permettant d'identifier la personne. La victime de l'usurpation d'identité reste vivante, et possède donc la faculté de défendre ses droits.

Les usurpateurs utilisent ensuite ces informations pour effectuer une ou des transactions en simulant l'identité de la personne fraudée. Par exemple, un fraudeur peut effectuer des appels téléphoniques ou faire des achats importants et diriger les frais vers la personne fraudée, il peut aussi retirer de l'argent du compte de banque de cette personne…. **[34]**

IV.2. Utilisation non légitime de l'information

Chacune des informations lâchées sur Internet peut paraître dérisoire, mais mises bout à bout elles permettent de dresser un profil parfois très complet d'une personne, et cela présente un risque d'atteinte à la vie privée du fait qu'il permet d'analyser avec précision le comportement des consommateurs.

Les informations collectées par les moteurs de recherches dans le cadre de leurs activités commerciales sont ensuite traitées et exploitées pour différentes finalités (offres de services, sécurité du système, publicités personnalisées, statistiques, etc.)

Un internaute inscrit sur un site de socialisation peut parfaitement diffuser des photos ou des commentaires sur un autre individu sans même que celui-ci soit inscrit sur le site. Enfin, en révélant des informations parfois très personnelles ou intimes (opinions politiques, religion, etc.) sur ces sites, les internautes s'exposent à une exploitation commerciale de leurs données par les gérants de sites ou leurs partenaires commerciaux. **[35]**

Donc comme on a vu, il y a de nombreuses manières d'utilisation malveillantes des informations touchant directement notre intimité, de ce fait, protéger sa vie privée n'est plus une question d'éthique.

V. Quelques techniques d'attaques

V.1. Les cookies (biscuits empoisonnées)

un cookie (aussi appelé plus rarement témoin) est défini par le protocole de communication HTTP[11] comme étant une suite d'informations envoyée par un serveur HTTP à un client HTTP, que ce dernier retourne lors de chaque interrogation du même serveur HTTP sous certaines conditions. **[36]**

Les cookies ont des implications importantes dans la vie privée et l'anonymat des utilisateurs du web dans lesquels peuvent être retracés des renseignements pertinents pour son commanditaire sur les comportements de l'utilisateur d'Internet.

[11] Littéralement le « protocole de transfert hypertexte », est un protocole de communication client-serveur développé pour le World Wide Web.

Ces « mini - bases de données » constituent une source d'atteinte à la vie privée de l'internaute et à son autodétermination sur les données qui la concerne.

Les cookies permettant de:

- **Identifier un navigateur**

Certaines applications des cookies permettent d'identifier votre navigateur au fil des consultations d'un même serveur et connaître précisément la liste des documents consultés.

- **Identifier un individu sur un site**

Identifier une personne ne veut pas forcément dire qui elle est. Si cette même personne est amenée à révéler son identité en remplissant un formulaire, l'administrateur du site Web considéré va non seulement savoir qui consulte son site mais, il va pouvoir le reconnaître par la suite et savoir, à chaque visite quels documents il aura consultés.

- **Traquer un individu sur plusieurs sites**

La possibilité d'insérer des publicités sur de très nombreux sites Web par le monde, lui permettant ainsi de savoir précisément le parcours d'un même internaute parmi ces différents sites. En exemple typique est l'entreprise DoubleClick [12] et ces célèbres cookies. **[12]**

V.2. Le Phishing

Le phishing ou hameçonnage, consiste pour les escrocs à envoyer au maximum d'utilisateurs un courrier électronique censément rédigé par un site Internet respectable.

Pour une raison ou pour une autre, le courrier demande à l'utilisateur de se connecter à son compte en cliquant sur le lien fourni, dont l'adresse apparente semble bien celle du site. En fait, l'adresse est un leurre et renvoie sur un faux site, copie de l'original. Quand l'utilisateur entre ses identifiants, l'escroc les récupère et peut ensuite les utiliser pour effectuer des transactions et procéder à des détournements de fonds. **[14]**

Il existe différentes variantes à l'hameçonnage. On notera le spear phishing et le in-session phishing qui sont respectivement l'hameçonnage ciblé (notamment à l'aide des réseaux sociaux) et l'hameçonnage de session (basé sur des pop-up [13] pendant la navigation).

[12] Une régie publicitaire (ciblage comportemental) sur Internet. Elle est rachetée le 14 avril 2007 par Google pour 3,1 milliards de dollars.

[13] Nouvelle Fenêtre de Navigateur s'ouvrant automatiquement au dessus de la Fenêtre de navigation actuelle de l'internaute, il utilisé en publicité pour afficher un nouveau bandeau sans surcharger une page.

Les attaques par hameçonnage sont le plus souvent dirigées vers les sites sensibles tels que les sites bancaires. Les sites de réseaux sociaux sont aujourd'hui également la cible de ces attaques. Les profils des utilisateurs des réseaux sociaux contiennent de nombreux éléments privés qui permettent aux pirates informatiques de s'insérer dans la vie des personnes ciblées et de réussir à récupérer des informations sensibles. **[15]**

V.3. Le Scam (Arnaque)

Le « scam » (« ruse » en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est issue du Nigéria, ce qui lui vaut également l'appellation « 419 » en référence à l'article du code pénal nigérian réprimant ce type de pratique.

L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur à besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

En répondant à un message de type scam, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euros s'il mord à l'hameçon et même la vie dans certains cas. **[16]**

V.4. Le logiciel espion (spyware)

Un logiciel espion (aussi appelé mouchard ou espiogiciel ; en anglais spyware) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

Un logiciel espion est composé de trois mécanismes distincts :

- Le mécanisme d'infection, qui installe le logiciel. Ce mécanisme est identique à celui utilisé par les virus, les vers ou les chevaux de Troie.

  Par exemple, l'espiogiciel Cydoor utilise le logiciel grand public Kazaa comme vecteur d'infection.

- Le mécanisme assurant la collecte d'information. Pour l'espiogiciel Cydoor, la collecte consiste à enregistrer tout ce que l'utilisateur recherche et télécharge via le logiciel Kazaa.
- Le mécanisme assurant la transmission à un tiers. Ce mécanisme est généralement assuré via le réseau Internet. Le tiers peut être le concepteur du programme ou une entreprise.

Le logiciel espion peut afficher des offres publicitaires, télécharger un virus, installer un cheval de troie (ce que fait WhenU.SaveNow, par exemple), capturer des mots de passe en enregistrant les touches pressées au clavier (keyloggers), espionner les programmes exécutés à telle ou telle heure, ou encore espionner les sites Internet visités. **[17]**

V.5. Les pixels invisibles

Ce sont des minuscules fichiers graphiques insérés dans un courriel ou dans une page Web pour surveiller un utilisateur à son insu.

En fait, un pixel invisible se met en marche lorsque nous téléchargeons une page Web. Il commence alors la collecte d'informations: adresse IP de l'ordinateur et autres informations nous concernant. Il peut alors connaître l'identité du fournisseur d'accès, puis envoyer un cookie pour analyser les habitudes de navigation.

D'ailleurs, selon une étude d'Intelytics de l'année 2009, 75% des sites commerciaux principaux utilisent les pixels invisibles pour nous traquer.

Pour cela Privacy Foundation a lancé Bugnosis, un logiciel qui permet de traquer ces drôles de pixels. **[37]**

V.6. Autres techniques d'attaques

V.6.1. Les chevaux de troie et les vers

On appelle « Cheval de Troie » (en anglais trojan horse) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur.

Un cheval de Troie (informatique) est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à l'ordinateur sur lequel il est exécuté en ouvrant une porte dérobée (en anglais backdoor), par extension il est parfois nommé troyen par analogie avec les habitants de la ville de Troie. **[18]**

Un cheval de Troie peut par exemple :

- voler des mots de passe ;
- copier des données sensibles ;
- exécuter tout autre action nuisible ;
- etc.

Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

L'objectif d'un ver n'est pas seulement de se reproduire. Le ver a aussi habituellement un objectif malfaisant, par exemple :

- Espionner l'ordinateur où il se trouve.
- Offrir une porte dérobée à des pirates informatiques .
- Détruire des données sur l'ordinateur où il se trouve ou y faire d'autres dégâts.
- Envoyer de multiples requêtes vers un serveur Internet dans le but de le saturer (déni de service). **[19]**

V.6.2. Adware

Un logiciel publicitaire (adware en anglais) est un logiciel qui affiche la publicité lors de son utilisation.

Le logiciel contient habituellement deux parties :
* une partie utile (le plus souvent un jeu ou un utilitaire) qui incite un utilisateur à l'installer sur son ordinateur.
* une partie qui gère l'affichage de la publicité.
Ces logiciels espions se renseignent sur les sites visités par un utilisateur, afin de mieux cibler le type de publicités à afficher, le plus souvent à travers des fenêtres pop-up. Les informations récoltées sont parfois stockées sur des bases de données à des fins commerciales. Il existe des logiciels intégrant des adware sans en avertir l'utilisateur. **[20]**
Pour plus de protection contre ces techniques d'attaques voir Annexe A.

VI. La protection de la vie privée sur internet

Cette section explique en quoi la protection de la vie privée est un enjeu important et de quelle manière l'Internet peut mettre en place la protection des informations personnelles. **[38]**

VI.1. Les niveaux de protection de la vie privée

- L'anonymat

C'est l'impossibilité (pour d'autres utilisateurs) de déterminer le véritable nom de l'utilisateur associé à un sujet, une opération, un objet

- La pseudonymat

Idem, sauf que l'utilisateur peut être tenu responsable de ses actes, c.à.d. il peut utiliser un pseudonyme au lieu de son vrai nom.

- La non-chaînabilité

C'est l'impossibilité (pour d'autres utilisateurs) d'établir un lien entre différentes opérations faites par un même utilisateur

- La non-observabilité

C'est l'impossibilité (pour d'autres utilisateurs) de déterminer si une opération est en cours.

Chaque entité qui utilise des données privés des utilisateurs doit respecter les principes suivants :

- La minimisation des données

Ça signifie que la seule information nécessaire pour compléter une application particulière devrait être collectée/utilisée (et pas plus).

C'est une application directe du critère de légitimité défini par la directive européenne sur la protection des données personnelles (Directive 95/46/EC).

- La souveraineté des données

Ça signifie que les données liées à un individu lui appartiennent, il devrait pouvoir contrôler comment elles sont disséminées.

C'est une extension de plusieurs législations nationales sur les données médicales qui considèrent que le dossier d'un patient lui appartient, et non pas au docteur qui le crée

ou le met a jour, ni a l'hôpital qui le stocke. Difficile a réalisé dans un monde ubiquitaire.

- Le consentement explicite

Ça signifie qu'avant de collecter les données personnelles d'un individu, il faut lui demander son autorisation et lui expliquer quelle utilisation sera faite de ses données.

- La transparence

Ça signifie que le système ne doit pas être considérer comme une boite noire dans laquelle l'individu doit avoir une confiance aveugle.

- L'imputabilité

Ça signifie que l'entité qui héberge les données personnelles doit les sécuriser au meilleur de ses moyens, et le cas échéant peut être tenue responsable (par exemple devant un juge) d'un bris de vie privée.

- Le droit à l'oubli

Ça signifie que sur la demande de l'individu, ses traces doivent être effacées. **[28]**

VI.2. Technologies de protection de la vie privée

VI.2.1. Privacy by design

C'est l'intégration de la problématique du respect de la vie privée dé la conception d'un système. Considère la question de la vie privée a priori, plutôt que de réagir a posteriori une fois que le système a été déployé et qu'on constate un bris de vie privée. **[28]**

- **Les principes fondamentaux**

- Proactive et non réactif

Le Privacy by Design est une approche qui se caractérise par des mesures proactives plutôt que réactives. Il prévoit et empêche des événements de la vie privée avant qu'ils se produisent. En bref, Privacy by Design vient avant le fait, non pas après.

- La vie privée comme un réglage par défaut

Privacy by Design vise à offrir le maximum de la vie privée en faisant en sorte que les données personnelles sont automatiquement protégées dans un système d'information et de gestion. Si une personne ne fait rien, leur vie privée demeure intact. Aucune action

n'est exigée de la part de l'individu pour protéger leur vie privée, elle est établie dans le système par défaut.

- La vie privée est intégrée dans la conception

Privacy by Design est intégré dans le design, l'architecture des systèmes et les pratiques commerciales.

Le résultat est que la vie privée devient une composante essentielle du fonctionnement. La vie privée fait partie intégrante du système, sans diminuer la fonctionnalité.

- Fonctionnalité complète (à somme positive)

Privacy by Design vise à répondre à tous les intérêts légitimes et les objectifs dans un jeu à somme positive «gagnant-gagnant » et non pas par une approche à somme nulle, où inutiles.

- Protection du cycle de vie complet

Privacy by Design, ayant été intégrés dans le système avant l'assemblage du premier élément alors des mesures de sécurité solides sont essentiels à la vie privée, du début à la fin. Cela garantit que toutes les données sont bien conservées puis détruits à la fin du processus en toute sécurité.

- Visibilité et transparence

Privacy by Design vise à assurer à tous les intervenants que toutes les pratiques sont exploitables selon les promesses et les objectifs énoncés. Ses composants et les opérations restent visibles et transparentes, pour les utilisateurs et les fournisseurs.

- Respect de La vie privée de l'utilisateur

La conception exige à des architectes de conserver les intérêts de l'individu le plus élevé en offrant des mesures telles que la vie privée forte par défaut. **[39]**

VI.2.2. Privacy Enhancing Technologies (PET)

PET est un ensemble de techniques et d'applications qui permettent à un individu de protéger ses informations personnelles pendant qu'il est en ligne.
Les "technologies de protection de la vie privée" regroupent un très grand nombre d'outils, mais ceux-ci demeurent complexes, peu standardisés et au final très peu utilisés. **[28], [40]**

- **Exemples des outils PET**

1) System de gestion d'identité

Les usages divers de l'Internet ont fait naître un peu partout dans le monde des comportements atypiques, tels que la multiplication des adresses électroniques, le recours aux pseudonymes dans les blogs, aux avatars dans les mondes virtuels, etc. Ces « identités multiples » sont plus difficiles à saisir qu'un numéro de passeport, de sécurité sociale ou de compte bancaire. **[21]**
Exemples: Microsoft passport, Single Sign-On (SSO), OpenID…

a) Windows Live ID

Windows Live ID (anciennement appelé Microsoft Passport) est un service qui permet d'utiliser une adresse de messagerie et un mot de passe uniques, appelés authentifiant, pour accéder à la plupart des sites et services de Microsoft ainsi que ceux de ses partenaires choisis.
Il permet d'enregistrer ces authentifiant (adresse de messagerie et mot de passe) à un site ou un service qui utilise Windows Live ID, ou au site Web Windows Live ID. Microsoft utilise cette identité unique pour aider à améliorer l'authentification de Windows Live ID et pour la protection contre les pourriels et l'utilisation malveillante du compte. **[22]**
Windows Live ID aide à protéger la vie privée et les informations personnelles de la manière suivante :

- Le service Windows Live ID collecte et traite les informations personnelles seulement pour les raisons suivantes :
    - Pour faire fonctionner un service d'authentification.
    - Pour aider à améliorer la sécurité.

- Pour le support technique.

- Le service Windows Live ID ne contrôle ni surveille les pratiques de confidentialité de tous les sites et services sur Windows Live ID. Les pratiques de confidentialité des sites individuels peuvent varier. Toutefois, tous les sites ou services Windows Live ID doivent être d'une déclaration de confidentialité validée. **[23]**

b) Single Sign-On (SSO)

L'authentification unique (ou identification unique ; en anglais *Single Sign-On* : SSO) est une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques (ou sites Web sécurisés).

Les objectifs sont multiples :

- Simplifier pour l'utilisateur la gestion de ses mots de passe : plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent.
- Simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire.
- Simplifier la définition et la mise en œuvre de politiques de sécurité. **[24]**

c) OpenID

OpenID est un système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites (devant prendre en charge cette technologie) sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID. Le modèle OpenID se base sur des liens de confiance préalablement établis entre les fournisseurs de services (sites web utilisant OpenID par exemple) et les fournisseurs d'identité (*OpenID providers*). Il permet aussi d'éviter de renseigner à chaque fois un nouveau formulaire en réutilisant les informations déjà disponibles. OpenID permet à un utilisateur d'utiliser un mécanisme d'authentification forte. **[25]**

Une faiblesse de ce système réside dans les risques de phishing ou d'hameçonnage. On peut en effet imaginer qu'une des fraudes du système OpenID consiste à détourner

l'utilisateur ou le fournisseur de service du fournisseur d'identité vers lequel il se dirige pour authentifier l'utilisateur. En dépit de ses faiblesses, OpenID, qui en est encore au stade expérimental, constitue un système d'identité numérique global très prometteur. **[41]**

2) Accès anonyme à des services

Les PETs permettant de communiquer de manière anonyme dans un réseau, c'est à dire en protégeant l'identité de l'envoyeur et/ou du receveur du message
Exemples : Mixnets, Onion Routing, Crowds, etc.

a) Mixnets

Concept introduit par Chaum en 1981 pour empêcher l'analyse de trafic. Le Mix est un routeur qui cache le lien entre les messages entrants et sortants par un mécanisme de chiffrement et de permutation des messages, pour faire face aux espions observant les communications échangées. Parmi ceux qui ont appliqué le Mixnets le Service de courriel anonyme (Mixmaster). **[42]**
Fonctionnement d'un Mix simple :

1. Reçoit en entrée plusieurs paires du type (message; adresse du destinataire) qui ont été préalablement chiffrées.
2. Déchiffre les messages.
3. Envoie en sortie les messages à leurs destinataires correspondants (possiblement chiffrés).

La figure suivante montre le fonctionnement d'un Mixnets :

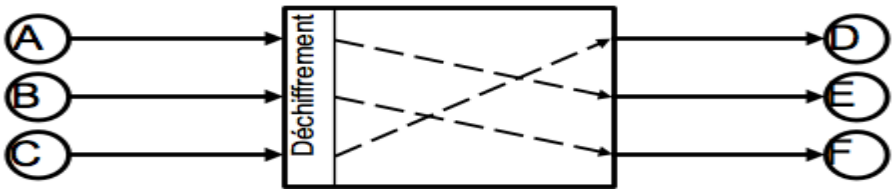

Figure I.1 : Mixnets moyenne d'accès anonyme **[42]**

b) Crowds

Protocole de communication anonyme qui protège l'anonymat de l'envoyeur d'un message en le routant de manière aléatoire vers des groupes d'utilisateurs similaires.

L'idée principale : cacher l'origine d'un message en le dispersant.

Fonctionnement de Crowds :

Initialisation : chaque nouvel utilisateur s'enregistre en tant que membre d'un groupe (appelé « Crowd ») en contactant le responsable du groupe. Quand un utilisateur rejoint un groupe, tous les membres du groupe en sont notifiés.

Le responsable du groupe est aussi chargé de la distribution des clés symétriques assurant la confidentialité entre paires de nœuds. **[42]**

c) Tor

The Onion Router ou Tor (le routage en oignon) est un réseau mondial décentralisé, organisés en couches, dont la tâche est de transmettre de manière anonyme les paquets TCP. Tout échange Internet basé sur TCP peut être anonymes en utilisant Tor. **[42]**

Tor fonctionne avec de nombreuses applications comme les navigateurs web, les clients de messagerie instantanée, les connexions à distance et tout un nombre d'application se basant sur le protocole TCP. **[43]**

3) Langages de préférence en termes de vie privée

Langages principalement basés sur le standard XML et utilisés pour permettre aux utilisateurs d'exprimer leurs préférences de confidentialité.

De même, ils facilitent la tâche des organisations pour exprimer des pratiques de confidentialité dans les serveurs Web **[44].** Le chapitre suivant détaillera ce type de langages.

VII. Conclusion

Au cours des dernières années les problèmes liés à la vie privée sur Internet sont devenus très importants aux yeux des utilisateurs.

Les usagers devraient savoir que tous les outils n'offrent pas des moyens efficaces de protéger la vie privée. Un gros désavantage tient à leur incapacité d'aborder la protection de la vie privée une fois les données sont collectées.

Pour cela de nombreux organismes internationaux se sont donc penchés sur la question, notamment le w3c (World Wide Web Consortium) qui a proposé le protocole P3P (Platform for Privacy Preference) qui sera éclairci dans le chapitre suivant.