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 :

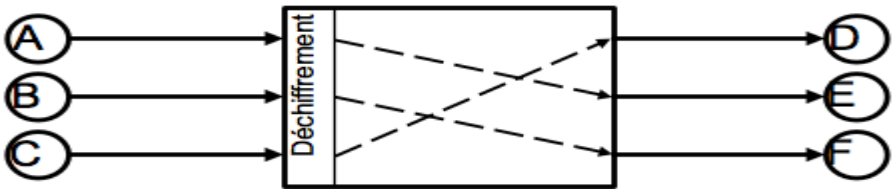

Figure I.1 : Mixnets moyenne d'accès anonyme **[42]**

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.