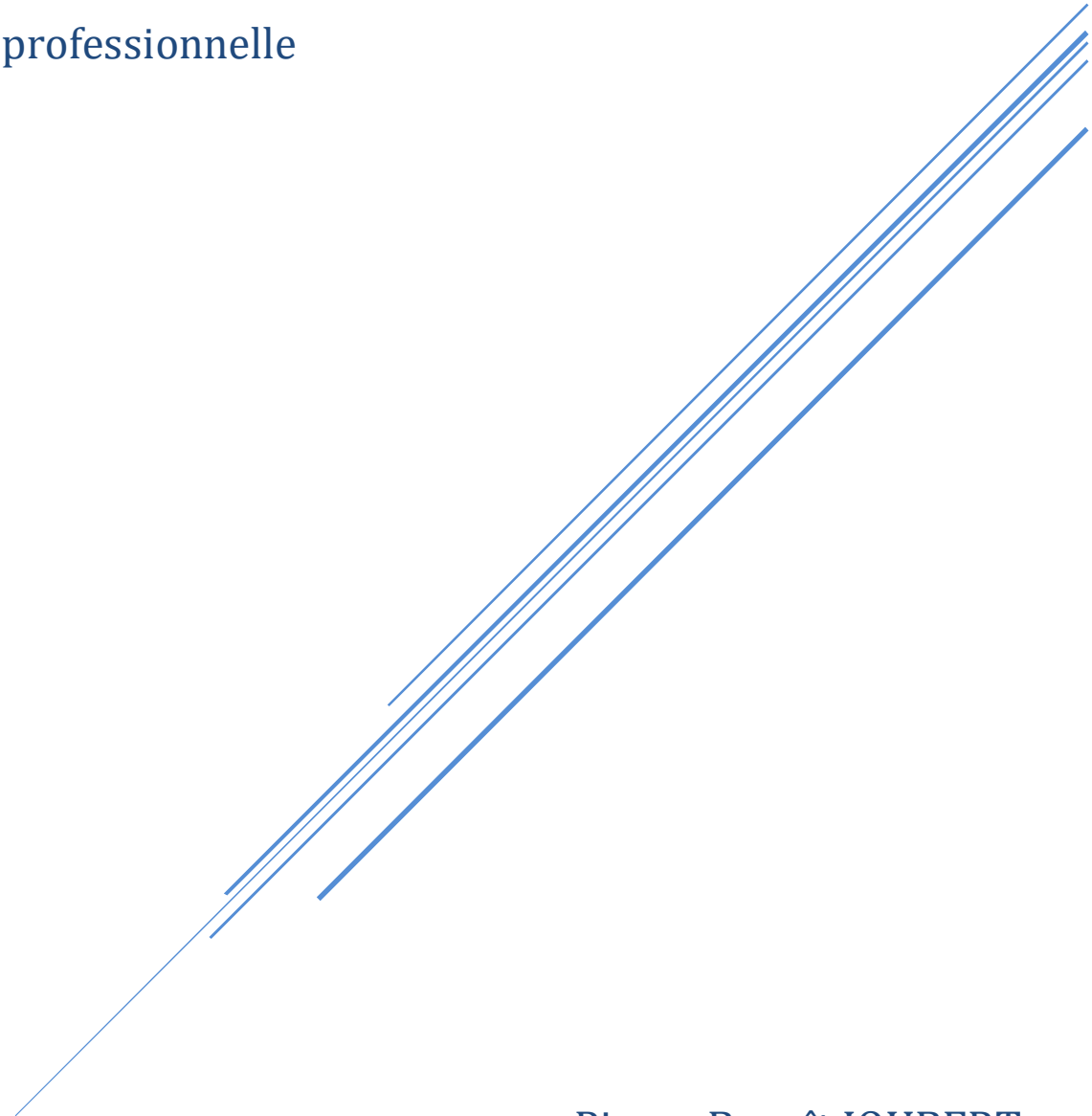
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

La liberté de l'information sur Internet

Thèse professionnelle



Pierre-Benoît JOUBERT
Manager des systèmes d'information 2015-2017

Remerciements

Je tiens à remercier Jean-Paul DOMERGUE (directeur des opérations) et Gilles PERES (responsable de site), mes deux tuteurs successifs, de m'avoir accueilli dans leurs équipes et accompagné dans cette expérience inoubliable qu'ont été ces 16 mois au sein du centre de recherche et développement d'une multinationale telle qu'Airbus Group.

Je remercie Olivier BUFFAT, responsable de formation au CESI, pour les échanges passionnants que nous avons eus autour du sujet de cette thèse professionnelle ainsi que de son encadrement tout au long de ma formation.

Je remercie l'ensemble de mes collègues de travail, du personnel et des intervenants du CESI, que j'ai eu la chance de côtoyer au cours de ces cinq ans et demi. Chacun, à sa façon, m'a permis d'arriver à l'aube de ma carrière professionnelle, en possession de multiples expériences et compétences professionnelles.

Je remercie Christophe BRAND, Bertrand DESPRES et Pierre-Yves PARIS d'avoir eu la gentillesse de prendre du temps afin de répondre à mes demandes d'interviews. Les discussions que nous avons eues se sont révélées au-delà de mes attentes.

Je remercie toutes les personnes qui ont accepté de compléter le sondage en ligne que j'ai fait circuler, avec une mention spéciale aux membres d'un forum (ils se reconnaitront).

Je remercie les personnes qui ont bien voulu relire ce document. C'est souvent dans le détail que se trouve la différence.

Enfin, je remercie toutes les personnes que j'aurais pu oublier dans les lignes ci-dessus. Mes plus plates excuses si c'est le cas, ce n'était pas dans mes intentions !

Résumé

Cette thèse, comme son titre l'indique, traite de la liberté de l'information sur Internet. C'est la notion de liberté numérique, regroupant différents domaines tels l'accès à l'information, son contrôle, la liberté d'expression, le droit à la vie privée…

De nombreux utilisateurs de technologies numériques n'ont pas encore pleinement conscience de l'ampleur des atteintes à ces droits fondamentaux qu'ils subissent au quotidien. Ces atteintes peuvent être de leurs propres faits, par ignorance de certains fonctionnements ou de leurs impacts, mais également contraints et forcés.

Cette thèse professionnelle n'a pas pour ambition de traiter l'intégralité des thématiques et des faits gravitant autour de ce sujet, loin de là ! La complexité de ce domaine d'étude et la densité des informations permettent d'aborder ce sujet de multiples façons. J'ai décidé de me concentrer sur un point focal : le droit à la vie privée et ses principales menaces.

À défaut de trouver un sujet de thèse dans le périmètre de mon entreprise, j'ai choisi de la réaliser sur un thème qui me tient à cœur depuis de nombreuses années, avec l'accord préalable de mon responsable de formation ainsi que de mon tuteur en entreprise.

Cette thèse a pour but d'être accessible à tous, aux néophytes comme aux utilisateurs avancés dans le domaine des technologies numériques.

Abstract

This thesis, as its name suggests, deals with the freedom of information on Internet. It is the concept of digital freedom, covering various domains : access to information, its control, the freedom of expression, the right to privacy…

Many users of digital technologies are not yet fully aware of the infringements of these fundamental rights that they endure every day. These breaches can be both, due to ignorance of system operation or the impacts on external forces.

This thesis does not purport to deal with the totality of the themes and the facts of this subject, far from it. The complexity of the subject and the high-density of the information mean this subject can be approached in a number of ways. This thesis focuses digital freedom and its main threats.

Having not found a thesis subject linked to the company's, the choice was made to conduct it on a subject that has been dear to the heart of the author for many years, with the prior consent of the author's training officer and tutor.

This thesis is intended to be accessible to everyone, to novices as well as to advanced users in the digital technologies domain.

Table des matières

Table des figures

1. Introduction

1.1 Contexte

La vie privée se définit par des faits et des informations, relevant du cadre privé, qu'une personne souhaite garder pour elle ou avoir la possibilité de les partager à sa convenance avec un petit nombre d'individus (cercle familial, amis proches…).

De nombreuses personnes crient à tort et à travers qu'elles n'ont rien à cacher aux géants du Net, au gouvernement… Justement si, leur vie privée ! Vouloir conserver une information pour soi ou avoir la possibilité d'en contrôler sa diffusion ne la rend pas pour autant illégale.

La vie privée fait partie des droits fondamentaux, figurant dans la déclaration universelle des droits de l'Homme. Régulièrement, des autorités administratives comme la « Commission nationale de l'informatique et des libertés » (CNIL) ou des organisations non gouvernementales telles que « Reporters sans frontières » (RSF) mettent en garde contre des atteintes à ces droits, qui augmentent d'année en année, parallèlement à l'évolution des technologies numériques dans nos vies quotidiennes.

Les données relatives à la vie privée sont une mine d'information couramment utilisée. Elles permettent de définir un profil de l'utilisateur le plus précis possible : ses habitudes, ses relations, ses centres d'intérêt… Et ce même si de nombreux textes de loi existent pour prévenir ce genre de pratiques abusives.

Il est possible que quelques points concernant le législatif aient changé au moment où vous lirez ces lignes, ce document ayant commencé à être rédigé voilà bientôt un an.

1.2 Problématique

Les technologies de l'ère du numérique apportent de nombreux outils au service des utilisateurs que nous sommes : ils facilitent notre vie au quotidien, nous permettent de communiquer, de partager des informations privées…

Ces nouvelles technologies ont aussi des contreparties : la manipulation et l'exploitation de nos données par des tiers.

La surveillance de masse et le profilage sont-ils compatibles avec la notion de vie privée ?

1.3 Hypothèses de travail

Deux choses me semblent importantes à souligner :

- L'accès aux informations sur Internet doit être contrôlé.

- Il n'est pas possible de contrôler l'information sur Internet à 100%.

Tout au long de cette réflexion, je vais essayer de vérifier ces deux hypothèses en regroupant des faits (par des informations issues de livres, d'Internet, …), et en analysant les différentes interviews et sondages que je serai amené à réaliser.

L'affirmation ou l'infirmation de ces hypothèses me permettra d'établir des préconisations pour répondre à la problématique posée.

1.4 Structuration du document

Ce document se décompose en plusieurs grandes parties : la première concerne l'état de l'art, la deuxième traite de l'analyse des différentes enquêtes de terrain que j'ai réalisées. Viennent ensuite les réponses aux hypothèses de travail, mes préconisations et la conclusion.

Certains documents n'ayant pas directement leur place dans le corps de cette thèse professionnelle seront placés dans les annexes.

2. État de l'art

2.1 Une brève note d'histoire

Le télégramme ainsi que le téléphone peuvent être considérés comme des précurseurs d'Internet.

Les premières évocations de l'Internet tel que nous le connaissons aujourd'hui sont du fait de Paul OTLET, en 1934, à travers son « Traité de documentation ». Il évoque alors la difficulté de stocker, classifier et partager une grande quantité d'informations sous format papier.

Ce n'est que dans les années 1950-60 que des recherches technologiques commencèrent pour donner le jour, 50 ans plus tard à l'Internet tel que nous le connaissons aujourd'hui.

C'est à la DARPA (« Defense Advanced Research Projects Agency »), sous tutelle du département de la défense américaine, que nous devons une grande partie du développement de l'Internet : les connexions point à point, l'évolution vers une architecture décentralisée pour prévenir de toute menace ennemie à l'encontre de l'intégrité du réseau, la naissance du réseau ARPANET en passant par le protocole de communication TCP/IP (encore largement utilisé de nos jours)... Nombreuses de ces évolutions sont encore utilisées aujourd'hui.

Ce réseau était, dans un premier temps, uniquement accessible au département de la défense américaine et à quelques universités, avant de devenir accessible aux centres de recherches scientifiques et plus tard au grand public. À l'origine, il n'était pas question d'utilisation commerciale.

En parallèle, d'autres réseaux et protocoles se développèrent un peu partout dans le monde. En France le projet Cyclades, au Royaume-Uni SERCnet puis JANET…

La DARPA recruta Vinton G. Cerf de l'université Stanford pour travailler sur l'uniformisation de tous ces réseaux. En 1973 une reformulation profonde avait été réalisée, permettant ainsi de

faire communiquer des réseaux utilisant des architectures et des protocoles différents entre eux. En 1983, TCP/IP devient le protocole officiel de l'échange des informations sur le réseau ARPANET.

En 1980, le réseau NFS (pour « National Science Foundation ») fusionna avec l'ARPANET. Rapidement, à la suite de l'extension massive de l'ARPANET, la DARPA se désengagea du développement direct au profit d'autres acteurs ; ses attributions initiales s'éloignant de plus en plus de leurs origines.

Dans le milieu des années 80, le terme « d'Internet » désignant cet ensemble de réseau mondial apparut.

Entre 1995 et l'an 2000, Internet connu une évolution fulgurante, principalement due à la démocratisation des ordinateurs personnels dans les foyers.

2010 marque l'avènement d'une nouvelle ère, connut sous le nom de « Web 2.0 », plaçant ce dernier au cœur de la société, le rendant de plus en plus incontournable dans la vie de tous les jours : les interactions sociales, les démarches administratives, l'avènement des objets connectés…

« Traité de documentation : le livre sur le livre, théorie et pratique », livre de Paul OTLET, éditions Mundaneum, 1934, page 428 à 431.

« L'Internet: Historique et évolution », site Internet planete.inria.fr, INRIA.

« Internet History Timeline: ARPANET to the World Wide Web », site Internet livescience.com, Live Science.

« Chronologie de l'histoire d'internet », site Internet sites.univ-rennes2.fr, Université Rennes 2.

« Internet History 1962 to 1992 », site Internet computerhistory.org, Computer History Museum.

« Brève histoire d'Internet », site Internet tuteurs.ens.fr, ENS/PLS.

« A Very Short History Of The Internet Of Things », site Internet forbes.com, Forbes.

2.2 Que se cache-t-il derrière ce terme : « Internet » ?

Pour beaucoup, le terme « Internet » signifie l'accès à une multitude d'informations, l'accès à un vaste réseau… Mais ce nom banalise la complexité qui se cache derrière !

2.2.1 Une toile d'araignée

Comme évoqué plus haut, Internet n'est pas composé d'un seul réseau, mais d'une multitude dialoguant entre eux. Il est souvent comparé à une toile d'araignée, de par son architecture décentralisée initiée par la DARPA.

Une requête circulant sur Internet peut emprunter un vaste nombre de chemins différents, certains plus rapides que d'autres, certains plus fiables… Il est question du routage de l'information.

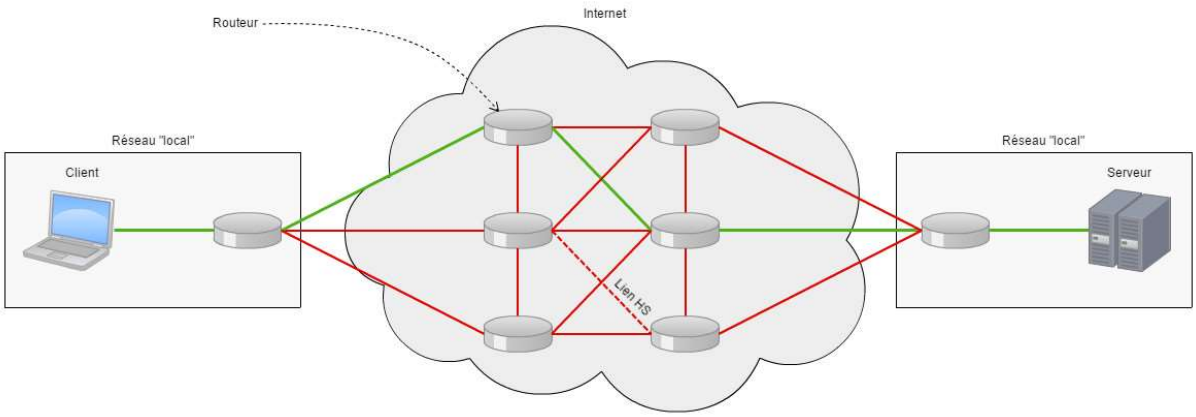


Figure 1 - Illustration du routage sur Internet

Si un lien est rompu ou si l'information met un temps trop important à parvenir à destination, elle empruntera un chemin différent.

2.2.2 Une histoire de routes, d'adresses et de noms

Afin de communiquer via Internet, toutes les machines qui s'y connectent possèdent une adresse. La fameuse adresse IP, dont nous entendons régulièrement parler au travers de l'actualité, de l'industrie hollywoodienne…

Il en existe deux types :

- IPv4, codée sur 32bits. Elle fait actuellement face à un problème de pénurie d'adresses disponibles.
- IPv6, codée sur 128bits. La longueur des adresses en IPv6 ne facilite pas leurs utilisations, mais elle permet de contourner le problème de pénurie connu de l'IPv4. Cette norme commence peu à peu à s'imposer dans le monde professionnel et chez les particuliers.

N. B. Pour faciliter les explications à venir, les exemples à suivre dans ce document utiliseront exclusivement des adresses en IPv4.

Une adresse IPv4 est composée de 4 nombres entiers, compris entre 0 et 255. Ce spectre d'adresses est divisé en de nombreuses plages. Une plage est un sous ensemble d'adresse IP, commençant de la même façon. Différents types de plages existent :

- Privées : Elles sont utilisées sur des réseaux locaux, par exemple chez vous, derrière la Box Internet fournie par votre fournisseur d'accès Internet (FAI).
  - 192.168.0.0/16
  - 172.16.0.0/12
  - 10.0.0.0/8
- Publiques :
  - 213.186.32.0/24
  - 87.98.216.0/24
  - 91.121.0.0/24

    - …
- Et bien d'autres types spéciaux (multidiffusion…).

Un organisme portant le nom de « Internet Assigned Numbers Authority » (IANA) a découpé en 256 plages les adresses IPv4, qu'elle a confiées à la gestion de différents organismes (RIPE en Europe, ARIN pour l'Amérique du Nord, APNIC pour l'Asie…). Ces organismes ont pour but de redécouper ces plages en sous plages pour les attribuer à d'autres organismes/entreprises… Ainsi, à partir de n'importe quelle adresse IP, il est possible de déterminer une information géographique (le pays, la région, le département, la ville, la rue…), l'entreprise finale qui l'exploite (Orange, SFR, OVH…) ainsi que différentes autres informations.

Afin d'être plus parlant pour les humains que nous sommes, il existe un annuaire mettant en relation les adresses IP (difficiles à retenir) avec des noms, plus précisément des noms de domaines. Il s'agit des « Domain Name Server » (DNS). Plusieurs dizaines de serveurs racines sont répartis à travers le Monde. Historiquement contrôlés par l'IANA (donc le gouvernement américain), aujourd'hui plusieurs pays y prennent part. Ces installations sont placées sous très haute surveillance.

Un utilisateur lambda qui veut aller sur son moteur de recherche favori, « Qwant » le bien nommé, effectuera les actions suivantes :

- Obtenir l'adresse IP associée au nom de domaine qwant.com
    - qwant.com → 194.187.168.99
- Préparer une requête
    - « Bonjour. Je voudrais, s'il vous plaît, consulter votre page d'accueil. »
- Envoyer la requête à 194.187.168.99
- Réception de la requête par un des serveurs de Qwant et analyse
    - « Bonjour. Vous êtes poli et votre requête me semble appropriée. Un instant, je vous prie. »

- Envoi d'une réponse
    - « J'ai trouvé l'information que vous cherchez, la voici. Bonne journée. »
- Réception de la réponse
    - « Merci. Bonne journée »
- Affichage de la page d'accueil dans le navigateur Internet de l'utilisateur

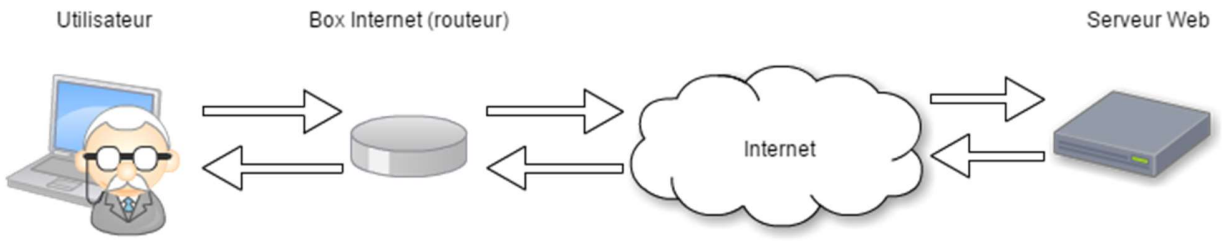


Figure 2 - Une requête « classique » vers un site Internet

Concernant l'information circulant via plusieurs réseaux, il est tout à fait possible qu'elle soit interceptée, voire même modifiée par un tiers, à des fins de contrôle de l'information (censures…) ou malveillantes (« Man in the Middle »…).

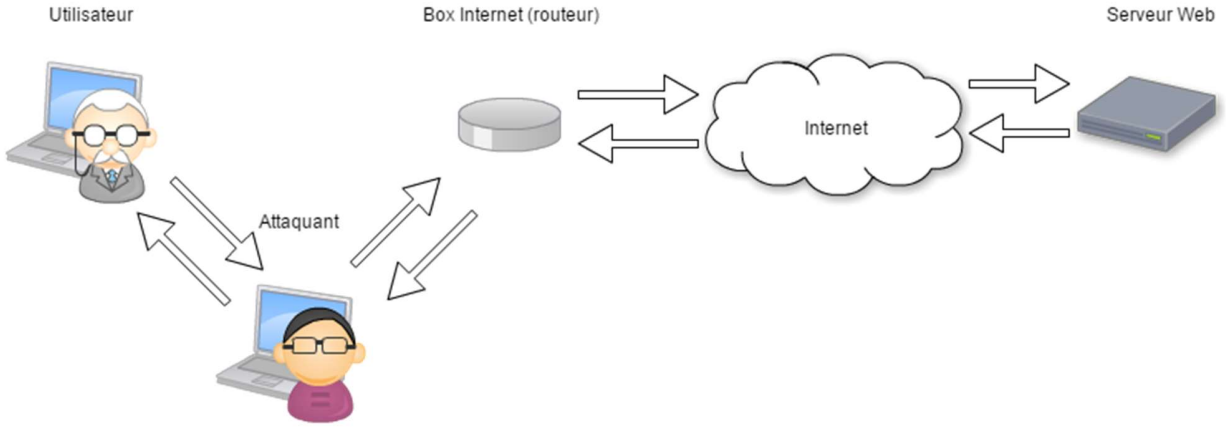


Figure 3 - Une requête vers un site Internet, interceptée par une attaque de type MITM

Pour éviter le recueillement d'information à partir de l'adresse IP source ou des possibilités évoquées si dessus, plusieurs solutions existent.

« Networking Basics: What You Need To Know », site Internet cisco.com, Cisco.

« How Does the Internet Work? », site Internet web.stanford.edu, Stanford University.

« 1.7.les réseaux », site Internet rmdiscala.developpez.com, Developpez.

« Number Resources », site Internet iana.org, IANA

« HTTP (HyperText Transfer Protocol) - Basics », site Internet ntu.edu.sg, Nanyang Technological University.

2.3 Protection des données et anonymisation

Par défaut, les informations transmises sur Internet circulent en clair. Ceci implique qu'un tiers se trouvant sur le chemin entre vous et la destination de l'information peut la lire. S'il s'agit d'informations basiques, comme consulter la météo ou les actualités, rien de très gênant. En revanche, acheter des biens ou des services en ligne, payer ses impôts, consulter son compte en banque… Autant d'informations gênantes si elles venaient à tomber entre de mauvaises mains. Garantir la confidentialité des informations qui transitent par Internet est un enjeu majeur.

Quand une information est émise sur Internet, sa source et sa destination sont connues. Il est ainsi possible de géolocaliser plus ou moins finement l'utilisateur, voir même de l'identifier clairement pour ce qui est du fournisseur d'accès Internet. Certains services se servent de cette géolocalisation pour limiter l'accès à leurs services. Ainsi, si l'on veut accéder à l'un d'eux dans un pays étranger, il est parfois nécessaire d'utiliser une des technologies suivantes.

2.3.1 Théorie

Depuis l'antiquité, l'Homme a trouvé des moyens pour faire parvenir des informations de façon à ce que seule la personne à qui elles étaient destinées puisse les voir/interpréter. Ces méthodes ont évolué au cours des siècles. Il s'agit là d'un combat de longue haleine, opposant les créateurs et les casseurs de codes.

2.3.1.1 Sténographie

La sténographie consiste à transmettre une information en la dissimulant avec une autre.

Un des premiers faits historiques connu remonte au début du Vème siècle av. J.-C., rapporté dans les écrits d'un historien grec du nom d'Hérodote, lorsque Xerxès 1er, roi des Perses,

commença à préparer une armée pour envahir la Grèce. Cette mobilisation devait rester secrète afin de prendre les Grecs par surprise. De nombreuses mesures étaient utilisées afin d'éviter toute fuite de l'information (fouille aux frontières, surveillance accrue…). Démarate, ancien roi de Sparte réfugié en Perse alerta les Grecs. Il envoya une tablette de cire avec des informations sans importance particulière écrites dessus. En réalité la tablette de cire avait été coulée en deux fois : une première couche, qui, une fois sèche reçut le message secret, puis une seconde qui reçut le message sans importance. Les deux couches ont simplement été superposées et soudées en faisant fondre le bord des deux tablettes. Malgré l'inspection minutieuse des gardes à la frontière, le message secret passa inaperçu et parvint aux Grecs à temps. Quatre ans plus tard, Xerxès aura la surprise de trouver les Grecs prêts à défendre leur territoire.

Depuis l'avènement de l'ère du numérique, ces techniques ont évolué. Il est techniquement très facile d'envoyer par email une photo… qui contient en réalité d'autres informations que la photo en question, mais il peut être difficile de le remarquer.

2.3.1.2 Chiffrement

Le chiffrement de données est en opposition avec le fonctionnement de la sténographie. Les informations chiffrées n'ont pas besoin d'être transmises de façon cachée de l'expéditeur au destinataire. Nous ne pouvons pas à proprement parler d'un « code secret ». En effet, le but du chiffrement est seulement de rendre une information compréhensible uniquement par l'expéditeur et le destinataire.

Il existe deux grandes familles de chiffrement : le chiffrement par transposition et le chiffrement par substitution.

Le premier est le plus ancien. Il consiste à redistribuer les lettres de l'alphabet dans lequel il est écrit. Il en résulte alors une anagramme. Cette méthode est peu fiable sur des messages de petite taille. Sur un mot comportant trois lettres, il existe seulement six solutions. En revanche,

sur un message de 35 caractères, il existe plus de 50 000 000 000 000 000 000 000 000 000 000 d'agencements possibles ! Un outil de chiffrement ancien utilisait cette technique : le Scytale. Il s'agissait d'un cylindre autour duquel venait s'enrouler une bandelette de cuir, lin… ou toute autre matière souple où il était possible d'écrire dessus. Une fois le message écrit sur le support, la bandelette était expédiée au destinataire. Le destinataire connaissant le diamètre précis du Scytale n'avait alors qu'à l'enrouler sur le sien et lire le texte en clair. Si le diamètre du Scytale était faux de quelques millimètres, le texte était illisible.

Figure 4 - Exemple de Scytale avec une bandelette de cuir enroulée dessus

Le chiffrement par substitution fait, quant à lui, appel, comme son nom l'indique, à des inversions fixes des lettres de l'alphabet. Le plus simple est le « chiffre de César ». Il consiste à décaler l'alphabet de « n » caractères vers la droite ou vers la gauche, « n » étant un nombre entier connu à la fois de l'expéditeur et du destinataire. Cette méthode est très simple à appliquer, mais également très faible sur le plan de la sécurité.

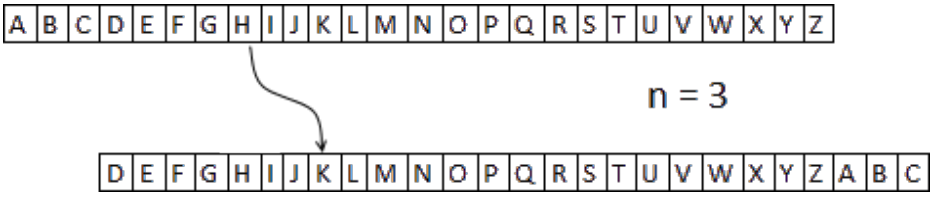


Figure 5 - Un exemple du « chiffre de César » où « n » = 3

Vinrent ensuite des méthodes de chiffrements un peu plus complexes, basés sur une redistribution des lettres de l'alphabet non linéaire.

Figure 6 - Exemple de substitution alphabétique, non linéaire

Bien que plus robuste que le « chiffre de César », cette méthode est devenue faillible depuis le IXe siècle apr. J.-C., grâce aux scientifiques arabes. Ils ont rapidement compris que, si la langue dans lequel le texte en clair avait été rédigé était connue, il suffisait d'utiliser la science des statistiques pour pouvoir le décrypter. Par exemple en français, le « A » représente environ 9,42% d'un texte, le « B » 1,02%, le « C » 2,64%... Il ne reste plus qu'à prendre le texte chiffré et essayer de faire des rapprochements.

Lettre	%	Lettre	%
A	9,42	N	7,15
B	1,02	O	5,14
C	2,64	P	2,86
D	3,39	Q	1,06
E	15,87	R	6,46
F	0,95	S	7,90
G	1,04	T	7,26
H	0,77	U	6,24
I	8,41	V	2,15
J	0,89	W	≈ 0,00
K	≈ 0,00	X	0,30
L	5,34	Y	0,24
M	3,24	Z	0,32

Figure 7 - Analyse des fréquences d'apparition des lettres dans un texte en français

Pour compenser les faiblesses des méthodes de chiffrement monoalphabétique, des méthodes polyalphabétiques firent leurs apparitions, dont une des plus connues, le « chiffre de Vigenére ».

Au XVe siècle, un savant Florentin du nom de Léon BATTISTA ALBERTI inventa le « chiffre de Vigenére », considéré durant plusieurs siècles comme indéchiffrable par les érudits du monde entier, grâce à l'utilisation d'un alphabet polyalphabétique.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 8 - Carré de Vigenére

Le carré de Vigenére est composé de 26 alphabets, chaque ligne étant décalée de « n » caractères avec la technique du « chiffre de César ». L'expéditeur et le destinataire doivent se mettre d'accord sur la valeur de « n » et sur l'utilisation d'une clé de chiffrement/déchiffrement

commune.

Prenons par exemple le mot clé ORANGE. Le chiffrement se fera donc sur 6 alphabets : la ligne 15 (O), 18 (R), 1 (A), 14 (N), 7 (G) et 5 (E). Pour chiffrer un texte, il suffit maintenant de lire la lettre que nous voulons chiffrer sur la première ligne, puis de chercher la lettre correspondante en descendant jusqu'à la ligne 15. Pour la deuxième lettre, idem, mais avec la ligne 18, la troisième lettre la ligne 1… Arrivé à six caractères chiffrés, on recommence au début de la clé de chiffrement. Il en résulte un message chiffré sur plusieurs alphabets, impossible à attaquer directement avec des analyses de fréquences.

Clé de chiffrement :	N	E	U	T	R	E	
Message chiffré :	Y	M	V	X	I	X	R
Message en clair :	À vous de le déchiffrer !						

Malgré qu'il y ait polémique sur la personne qui a cassé le « chiffre de Vigenére » en premier, il s'avèrerait que le mérite revienne à Charles BABBAGE, citoyen anglais, en 1854. L'utilisation d'un chiffrement polyalphabétique rend toute tentative de déchiffrement par analyse des fréquences inutile. Charles BABBAGE a réussi à le casser en se concentrant sur la découverte de la clé de chiffrement, en observant la répétition de probables répétitions dans le texte chiffré et en complétant les inconnues par des suppositions.

Dans les années 20, un Allemand du nom de Arthur SCHERBIUS commença à réfléchir à une machine de chiffrement révolutionnaire : Enigma.

Le fonctionnement en est assez simple. La machine est composée de trois rotors, de gros disques comportant 26 connexions électriques de chaque côté. Chaque contact d'une face est relié à un autre de l'autre côté, mais jamais directement à celui d'en face. L'expéditeur et le destinataire devront donc régler les rotors dans le même ordre et la même position afin de pouvoir chiffrer et déchiffrer les messages qu'ils s'échangent. Plus tard, afin d'augmenter la

sécurité qu'offrait cette machine, diverses modifications ont été apportées : un tableau de câblage afin d'inverser des lettres ainsi que deux rotors supplémentaires.

Cette machine servira quelques années plus tard à chiffrer toutes les communications allemandes pendant la deuxième guerre mondiale. Les opérateurs en charge du chiffrement des communications recevaient chaque mois un carnet comportant les clés de chiffrement à utiliser. Un code par jour.

Figure 9 - Une machine Enigma, utilisée pendant la deuxième guerre mondiale

Alan TURING et son équipe ont cassé ce chiffrement et permis de raccourcir la deuxième guerre mondiale de plusieurs années, grâce à un des premiers ancêtres de l'ordinateur moderne. Ce qui est beaucoup moins mis en avant dans cet exploit sont les recherches d'un scientifique polonais du nom de Biuro SZYFROW et des services de renseignement français. Sans bon nombre d'éléments transmis aux Anglais avant l'invasion de la Pologne, Enigma n'aurait peut-être pas été compromise.

Un des plus gros problèmes dans l'art du chiffrement est l'échange des clés entre l'expéditeur et le destinataire. Afin de garantir un maximum de sécurité, une clé de chiffrement ne peut pas

être utilisée plus d'une fois. Il faut donc constituer un stock suffisant de clés et en faire parvenir une copie au destinataire, pour qu'il puisse prendre connaissance des messages que nous lui enverrons par la suite. Le télégraphe, le téléphone, un coursier… Rien ne nous garantit que les clés transmises par ces biais ne soient pas interceptées. Cette méthode n'est donc pas la bonne.

Ce problème à longtemps était considéré comme insoluble. Il fallut attendre la deuxième partie du XXe siècle pour y apporter une solution. Whitfield DIFFIE et Martin HELLMAN commencèrent à élaborer différentes théories et recherches sur le sujet du chiffrement asymétrique. La mise en pratique telle que nous l'utilisons au quotidien dans nos échanges numériques est due à trois chercheurs du MIT (« Massachusetts Institute of Technology »), Ronald RIVEST, Adi SHAMIR et Leonard ADLEMAN.

Le chiffrement asymétrique, comme son nom l'indique, utilise deux clés. Une pour chiffrer et l'autre pour déchiffrer. Celle qui est utilisée pour chiffrer ne peut pas le déchiffrer et inversement, la clé utilisée pour déchiffrer ne peut pas chiffrer. Il est ainsi possible de mettre en ligne la clé destinée à chiffrer, accessible à tous. Une personne voulant m'envoyer un message chiffré pourra ainsi le faire avec cette clé dite « publique ». La seule personne pouvant le déchiffrer est la personne en possession de la clé privée, moi.

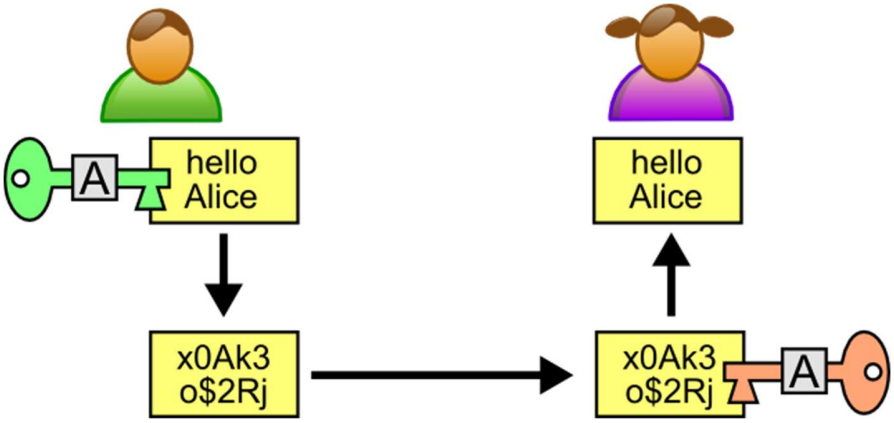


Figure 10 - Exemple montrant le principe de chiffrement asymétrique

2.3.2 Pratique

2.3.2.1 TLS

Le TLS (ou SSL) permet d'authentifier les deux parties en communication, de chiffrer les données et contrôler l'intégrité des données qui sont échangées. Il est couramment rencontré sur Internet, avec le protocole HTTPS.

De nos jours, Internet fait partie intégrante de nos vies : démarches administratives, banques, commerces en ligne, réseaux sociaux… Vos informations circulent dans ce vaste réseau mondial de l'information. TLS est là pour vous garantir que vous êtes en train de dialoguer avec la bonne personne et que vos données seront lisibles uniquement par le destinataire à qui elles sont adressées.

2.3.2.2 VPN

Un VPN (« Virtual Private Network ») permet d'interconnecter plusieurs machines ou réseaux entre eux de façon virtuelle, afin de reproduire un fonctionnement le plus proche possible d'un environnement physique. Ainsi, une entreprise peut par exemple interconnecter deux sites distants via Internet afin de partager différentes ressources réseau (stockages de fichiers, imprimantes, VoIP…) de façon la plus transparente possible pour l'utilisateur final. Un VPN peut également permettre à un utilisateur nomade de se connecter à distance au réseau de son entreprise.

À l'image du Wi-Fi, faisant abstraction de la sécurité d'une interconnexion physique maitrisée, les données transitant par un VPN (via Internet…) sont chiffrées, afin de garantir au maximum

leur confidentialité.

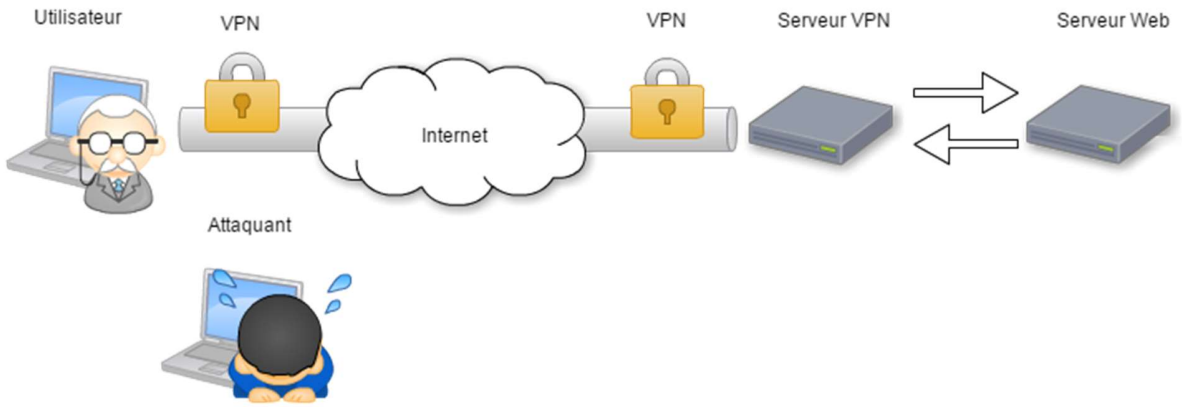


Figure 11 - Une requête « classique » vers un site Internet, en utilisant un VPN

Prenons deux bâtiments séparés par une route. Si un employé envoie un document sous forme d'un avion en papier à son collègue d'en face, il peut être intercepté et lu par n'importe qui. En revanche, si un tuyau PVC est préalablement installé entre les deux fenêtres, les personnes dans la rue vont savoir qu'il se passe quelque chose dans ce tuyau, mais seront incapables d'en affirmer la nature et encore moins les détails.

Un utilisateur nomade pourra ainsi se connecter au réseau de son entreprise via Internet (accéder aux données, téléphoner, surfer sur Internet…) et ce même via une connexion Wi-Fi ouverte et peu sécurisée comme il n'est pas rare d'en trouver dans des hôtels, restaurants…

2.3.2.3 Tor (alias le « Deep Web »)

Cette technologie a vu le jour dans les années 2000, bien que des recherches remontent jusque dans les années 1990, dont la DARPA en 1997. Ce projet est aujourd'hui maintenu par une société à but non lucratif : The Tor Project. Elle est financée par des dons, des organismes gouvernementaux…

Tor est un acronyme de « The Onion Router ». Il s'agit d'un réseau opérant grâce à Internet qui a pour but de rendre anonyme les connexions d'un utilisateur. Comme son nom l'indique, il fonctionne par couche : chaque utilisateur se connectant à ce réseau devient un nœud de routage. Toute connexion effectuée sur ce réseau fera transiter les informations par un nombre indéterminé de nœuds « utilisateur » avant d'emprunter un nœud de sortie.

Figure 12 - Une requête « classique » vers un site Internet, en utilisant le réseau TOR

Chaque connexion est chiffrée, empêchant son interception à des fins malveillantes par une attaque de type « man in the middle » entre les nœuds, d'une façon similaire au fonctionnement d'un VPN. Une fois l'information ayant quittée le nœud de sortie, sa véritable source est inconnue et remplacée par celle du nœud de sortie, garantissant ainsi son anonymisation.

Ce « monde parallèle » a parfois mauvaise presse. En effet, de nombreux sites « underground » y ont trouvé refuge : vente en ligne de substances illicites, vente d'armes, trafics d'êtres humains, pédopornographie… Le tableau est sombre. La montée en puissance des cryptomonnaies comme le Bitcoin y contribue grandement. En plus de voir leurs identités protégées par Tor, les transactions financières sont elles aussi anonymisées.

Ce réseau permet également aux personnes de communiquer librement, et ce malgré le fait qu'ils résident dans des pays aux mains de régimes totalitaires, où la censure d'Internet et la répression est courante.

Certaines informations révélées par Edward SNOWDEN laissent à penser que la NSA serait en

mesure d'exploiter des données transitant sur le réseau Tor, mais de façon limitée. Il est fait état de lever l'anonymat et le chiffrage des échanges d'une fraction d'utilisateurs et de façon aléatoire car il est impossible de cibler une personne en particulier. Il s'agit là certainement d'une question de temps avant la possibilité d'une éventuelle surveillance de masse, grâce à l'évolution des technologies, de la puissance de calcul des ordinateurs…

« Histoire des codes secrets », livre de Simon SINGH, éditions Le livre de poche, 2001.

« La stéganographie », PDF publié sur le site Internet univ-orleans.fr, Université d'Orléans.
« Chiffrement et Stéganographie », site Internet korben.info, Korben.
« Steganography: Hiding Data Within Data », site Internet garykessler.net, Gary C. Kessler.

« Classical Cryptography », site Internet cs.uri.edu, University of Rhode Island.
« Transposition Ciphers », site Internet cs.utexas.edu, University of Texas at Austin, Department of Computer Science.

« The Caesar Cipher », site Internet cs.trincoll.edu, Trinity College.
« The Caesar Cipher and Modular Arithmetic », site Internet math.stonybrook.edu, Stony Brook University, Mathematics Department.

« Cracking Classic Ciphers », site Internet rivier.edu, Rivier University.
« Classical Ciphers and Frequency Analysis Examples », site Internet sandilands.info/sgordon/, Steven GORDON.

« Vigenere Cipher », site Internet nctm.org, National Council of Teachers of Mathematics.
« The Vigenère Cipher Encryption and Decryption », site Internet cs.mtu.edu, Michigan Technological University, Computer Science Department.
« The Vigenère Cipher: Frequency Analysis », site Internet cs.mtu.edu, Michigan Technological

University, Computer Science Department.

« Enigma Cipher Machines », site Internet cryptomuseum.com, Crypto Museum.

« The Enigma cipher machine », site Internet codesandciphers.org.uk, Codes and Ciphers.

« Asymmetric-Key Cryptography », site Internet cs.cornell.edu, Cornell University, Department of Computer Science.

« Past, present, and futur methods of cryptography and data encryption », PDF publié sur le site Internet eng.utah.edu, The College of Engineering at the University of Utah.

« The Enigma cipher machine », site Internet codesandciphers.org.uk, Codes and Ciphers.

« The NSA and Weak-DH », site Internet lawfareblog.com, Lawfare.

2.4 Mondialisation des informations et législations locales

Grâce à Internet, la distribution de l'information est passée de supports locaux (journaux, courrier, téléphone…) à un support international. L'information n'est plus bornée à une localisation géographique.

De même, plus besoin d'avoir une carte de presse ou de travailler pour une chaine de télévision pour se faire entendre de façon « massive ». Quelques clics suffisent pour obtenir un espace d'expression.

Malgré cela, l'encadrement juridique existe toujours au niveau de chaque pays, de façon indépendante, avec des mesures et des sanctions propres à chacun. S'il n'est pas légal dans son pays d'origine de publier/accéder à un certain type de contenu, il suffit de passer par un autre pays (VPN, proxy, Tor…).

« Economie numérique et mondialisation : des vecteurs de croissance et de liberté ? », site Internet arcep.fr, ARCEP.

« Mondialisation et Internet », site Internet henricapitant.org, Association Henri Capitant.

2.5 Profilages, censures, filtrages et désindexations

À travers le monde, de nombreux gouvernements/régimes maitrisent l'information par la censure. Chine, Iran, Cuba… Autant de noms qui nous viennent directement à l'esprit quand on aborde ce sujet. Les plus oppressifs étant l'Érythrée, la Corée du Nord et l'Arabie Saoudite. La France en fait également partie, mais à un niveau bien plus modéré. Au contraire, d'autres pays défendent la « neutralité de Net » : Pays-Bas…

2.5.1 Profilages

De nombreux services et logiciels de qualité sont aujourd'hui facilement trouvables sur Internet. Malheureusement, il est rare qu'une société fasse vraiment quelque chose de 100% gratuit. En effet, il faut bien qu'elle tire une source de revenus quelque part.

Google, Facebook, Amazon, Microsoft… Et bien d'autres sociétés très connues font usage du profilage des utilisateurs pour tirer des revenus. Le profilage peut prendre plusieurs apparences. Le plus courant consiste à suivre la navigation d'un utilisateur afin de dresser un profil lui correspondant le plus possible : sur quels sites Internet il va, quels produits il achète, de quoi parle-t-il dans les emails qu'il envoie… ? Une fois ce profil dressé, il est très facile de lui proposer des publicités ciblées, et ainsi augmenter le nombre de chances que l'utilisateur clique dessus. Amazon étant un site de e-commerce, a un intérêt direct, Google et Facebook vendent des emplacements publicitaires… Et nous ne parlons même pas de la revente des renseignements à d'autres entreprises !

Sur l'année 2015, Facebook a dépensé 6,225 milliards de dollars (datacenters…) pour 1,591 milliard d'utilisateurs. On peut donc en déduire qu'un utilisateur rapporte au moins 3,91$.

Nous en sommes là aujourd'hui. Imaginez quelle ampleur cela pourrait prendre dans 10, 20 ou

30 ans avec l'avènement d'un monde connecté encore plus omniprésent dans nos vies ! Trackers d'activité, Smartphones… Les données qu'il est possible de recueillir sur notre vie quotidienne se comptent par centaine et les limites de notre vie privée vont en s'amenuisant.

Un adage est couramment employé dans le monde du logiciel libre : « lorsqu'un service est gratuit, c'est vous le produit ». Il est probablement plus vrai que ce que l'on pense.

2.5.2 Censures et filtrages

2.5.2.1 Érythrée + + + + +

Figurant parmi l'une des dictatures les plus sanglantes d'Afrique, l'Érythrée arrive en première tête du classement des pays appliquant la plus forte censure. Pas d'accès mobile à Internet. Moins de 1% de la population y a accès, via des lignes commutées. Les fournisseurs d'accès Internet ne font que distribuer à l'intérieur du pays, la connexion vers l'extérieur du pays étant contrôlée par le gouvernement. En plus de la censure de contenus, une répression sévère est appliquée. Toute information divulguée ne suivant pas les directives de l'État risque de mener à une peine de prison, voire même à la peine de mort. Même les journalistes travaillant pour l'État ont peur que leurs propos soient mal perçus et déplaisent au régime du président Isaias AFEWERKI.

2.5.2.2 Corée du Nord + + + + +

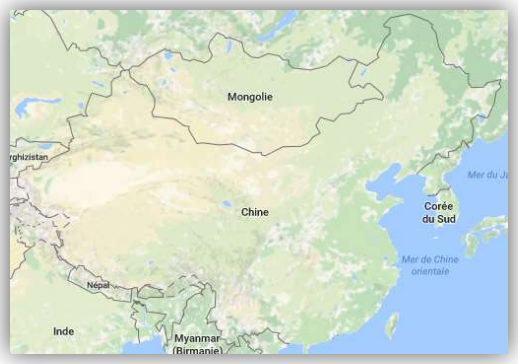
L'accès à Internet est limité à certains hauts-fonctionnaires triés sur le volet et probablement contrôlés de surcroit. Certaines institutions d'état (écoles, hôpitaux…) ont tout de même accès à l'Intranet du pays, fournissant des services approuvés et

contrôlés par l'état. Malgré l'accès au réseau mondial très limité, la répression est une réalité face à la libre expression, bien que la liberté de presse soit autorisée dans l'article 53 de la constitution du pays (probablement si elle est en accord avec le régime en place).

2.5.2.3 Arabie Saoudite + + + +

Bien que l'accès à Internet soit beaucoup plus répandu dans le pays qu'en Érythrée et en Corée du Nord, le gouvernement surveille de près la population. La répression est en hausse depuis le Printemps arabe. Toute forme de critique sur le gouvernement, la charia ou la religion d'État (l'Islam) est passible de peine de prison, peine de mort… La loi du pays a d'ailleurs été révisée en 2008 pour permettre à la Cour pénale spécialisée d'entendre des témoignages (non contestables) sans la présence de l'accusé et de son avocat. En 2014, le gouvernement a reconnu surveiller activement (en autre) la plateforme de partage de vidéos YouTube, afin de condamner tout appel à l'opposition.

2.5.2.4 Chine + + + +



La Chine avec ces 642 millions d'usagers (en comparaison, 47 millions en France) représente à elle toute seule environ 22% des Internautes de la planète, et ce malgré la « Grande muraille numérique », nom donné en référence à la grande muraille de Chine, monument historique mondialement renommé.

Il s'agit d'un système de filtrage mis en place dans les années 2000, suite à différents événements politiques opposant le parti communiste chinois et le parti démocratique chinois. Ce système est ainsi censé protéger le pays de l'influence des pays occidentaux (Capitalisme vs

Communisme…).

Il fonctionne en empêchant le routage vers certaines adresses IP internationales. Il repose sur un système de pare-feu « classique » et de proxy au niveau des passerelles Internet. Il utilise également l'empoisonnement de DNS afin de rediriger des sites internationaux vers d'autres « made in China », contrôlés en partie par le gouvernement (Google vers Baidu, Facebook vers Renren…). Il se compose également de censeurs, humains et technologiques, afin de repérer toutes transmissions d'informations qui pourraient se révéler dangereuses pour le gouvernement (critiques, complots…).

Contrairement aux pays précédemment cités, il est possible de contourner ce filtrage. En effet, de multiples articles trouvables en ligne font état d'une possible utilisation de technologies anonymisantes (tel que Tor, divers VPN…) par le grand publique.

2.5.2.5 France + +

La France a également été signalée par RSF comme étant un pays « sous-surveillance », ayant des lois liberticides concernant la liberté d'accès à l'information sur Internet. Depuis novembre 2014, un site Internet peut être bloqué sur demande d'une autorité administrative, sans demander l'accord préalable d'un juge. Les fournisseurs d'accès à Internet opérant sur le territoire national reçoivent alors l'ordre d'en interdire l'accès aux Internautes. Ces mesures ont été renforcées lors de l'adoption de l'état d'urgence en novembre 2015, notamment pour les sites faisant l'apologie du terrorisme, appel à la haine…

En 2015, Bernard CAZENEUVE a annoncé que 283 sites ont été bloqués, au cours du forum international sur la cyber sécurité de Lille.

Des lois sur le renseignement ont également été adoptées durant cette même période. Ce sujet sera plus amplement détaillé dans une partie dédiée à l'actualité.

2.5.2.6 Pays-Bas

Les Pays-Bas ont également eu recours à l'utilisation du blocage filtrage pendant plusieurs années. Depuis 2012, la neutralité du Net fait partie de la constitution du pays : pas de censure, pas d'analyse du trafic, pas de priorisation de paquets...

2.5.3 Moteurs de recherches

Aujourd'hui, les moteurs de recherches sont une « porte d'entrée » sur Internet. Il n'est pas rare qu'un utilisateur utilise un de ces services afin d'accéder à un site, et ce même s'il connait déjà sa cible. Ils deviennent l'annuaire, la carte routière et le GPS de ce monde numérique. Essayez de passer une journée sans en utiliser un et vous verrez la dépendance que nous avons envers eux.

L'indexation des sites Internet et l'exploitation des données ainsi recueillies sont utilisées la majeure partie du temps par les moteurs de recherches comme bon leur semble. Ces entreprises (Google, Bing, Yahoo…) sont souvent aussi puissantes financièrement (voir parfois plus) que des états ; difficile de faire pression sur eux.

La pratique du déréférencement est monnaie courante, par exemple pour les liens partageant illégalement des contenues sous copyright, ou tout autre contenu jugé inapproprié sur Internet (téléchargements illégaux, appelant à la haine…).

En France, depuis 2014, la CNIL impose aux moteurs de recherche un « droit à l'oubli ». Ceci permet à une entité (particulier, entreprise…) de demander la désindexation de certains

contenus liés à son nom. Les moteurs de recherche ne sont pas toujours très coopératifs.

« surveillance://: Les libertés au défi du numérique : comprendre et agir », livre de Tristan Nitot, aux éditions C&F Éditions, 2016.

« Le profilage des individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données », PDF publié sur le site Internet coe.int, Conseil de l'Europe.
« Le profilage et la publicité ciblée », PDF publié sur le site Internet cai.gouv.qc.ca, Commission d'accès à l'information du Québec.
« Online Profiling », site Internet computerworld.com, Computer World.
« Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law », PDF publié sur le site Internet ivir.nl, Institute for Information Law.

« Les 10 pays qui exercent la censure la plus forte », site Internet cpj.org, Committee to Protect Journalists.
« Censure du Net », site Internet laquadrature.net, la Quadrature du Net.
« Chine : la Grande Muraille électronique à son apogée », site Internet 12mars.rsf.org, Reporters sans frontières.
« Les Pays-Bas inscrivent la neutralité du Net dans la loi », site Internet lemonde.fr, le Monde.

« Google, le blacklistage et la censure », site Internet infonum.iut.u-bordeaux-montaigne.fr, IUT Bordeaux Montaigne.

2.6 Droit à la vie privée

Bien que parfois négligé ou peu respecté, le droit à la vie privée, numérique ou non est abordé dans de nombreux textes. Parfois ils ont une valeur juridique directe, tandis que d'autre fois, secondaire.

2.6.1 Déclaration universelle des droits de l'homme, article 12

La déclaration universelle des droits de l'homme a été adoptée le 10 décembre 1948 à Paris. Elle n'a pas de portée juridique en soi, il s'agit seulement d'une proclamation de droits.

> *« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »*

Il est clairement fait état de la protection de la vie privée, correspondance… Le numérique n'est pas clairement cité, car en 1948 la question ne se posait pas. Aujourd'hui, il est difficilement dissociable de la vie d'un individu résidant dans un pays économiquement développé. Il va de soit que ce texte s'y applique également par extension.

2.6.2 Convention européenne des droits de l'Homme, article 8

La convention de sauvegarde des droits de l'Homme et des libertés fondamentales, souvent appelée convention européenne des droits de l'homme a été adoptée le 4 novembre 1950 par les états membres de l'Union Européenne. Elle est rentrée en vigueur 3 ans plus tard, en 1953.

Il s'agit cette fois-ci d'un texte ayant une réelle valeur juridique, pour les états de l'Union Européenne.

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

La première partie de la citation reprend une partie de l'article 12 de la déclaration des droits de l'Homme. La deuxième partie apporte un complément, autorisant un état à y contrevenir sous certaines conditions. Il faut qu'une loi soit adoptée dans le pays en question, dans un but précis et défini. La loi renseignement en France en est un exemple.

2.6.3 Charte des droits fondamentaux de l'Union Européenne, articles 7 et 8

La Charte des droits fondamentaux de l'Union Européenne a été adoptée le 7 décembre 2000. Comme la convention européenne des droits de l'Homme, elle a une portée juridique pour les pays membres de l'Union Européenne. Le traité de Lisbonne apporte certaines précisions d'application concernant certains domaines. La France n'en fait pas partie.

> *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »*

Idem que dans l'article 8 de la convention européenne des droits de l'Homme, il s'agit d'une référence à l'article 12 de la déclaration des droits de l'Homme.

« Toute personne a droit à la protection des données à caractère personnel la concernant.

Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

Cet article fait référence à l'utilisation des données des utilisateurs. Il est précisé que le stockage et l'utilisation des données doivent être faits en prenant les mesures de sécurité nécessaires (chiffrement si données sensibles, déclaration à la CNIL…) et avec l'accord préalable de l'utilisateur (hormis si une loi l'autorise explicitement dans un cadre précis). Certaines affaires font un peu de bruit, de temps à autre : Google, Facebook… Il accorde également à l'utilisateur de pouvoir accéder aux données le concernant et de pouvoir y apporter des modifications si besoin est.

2.6.4 Déclaration commune des autorités européennes, articles 6, 7 et 8

La déclaration commune des autorités européennes a été adoptée le 25 novembre 2014 à Paris. Il s'agissait de réaffirmer les valeurs communes de l'Europe et de proposer des actions concrètes pour élaborer un cadre éthique Européen.

Le G29 est un organe consultatif européen indépendant. Il a pour but d'apporter ses conseils à la commission Européenne, de promouvoir une application uniforme des directives adoptées en la matière, ainsi que de proposer des recommandations au grand public.

« La surveillance secrète, massive et indiscriminée de personnes en Europe, que ce soit par des acteurs publics ou privés, qu'ils agissent au sein des États membres de l'Union ou ailleurs, n'est pas conforme aux Traités et législations européens. Elle est inacceptable sur le plan éthique. »

Cet article condamne la surveillance de masse au sein des états membres de l'Union Européenne, qu'il s'agisse d'une entreprise privée (fournisseur d'accès à Internet…) ou bien par l'état lui-même.

« L'accès à des données à caractère personnel aux fins de sécurité n'est pas acceptable dans une société démocratique dès lors qu'il est massif et sans condition. La conservation, l'accès et l'utilisation de données par les autorités nationales compétentes doivent être limités à ce qui est strictement nécessaire et proportionné dans une société démocratique. Elles doivent être soumises à des garanties substantielles et effectives. »

Ici aussi il est question de surveillance de masse. Elle est condamnée, même si elle est utilisée à des fins de sécurité, si elle est « massive et sans condition ». La loi renseignement est tolérable du point de vue de cet article, étant inscrite dans un cadre légal, stipulant une durée maximale de rétention des données, leurs natures, la possibilité d'y accéder sur décision de justice uniquement…

« Le traitement de données personnelles dans le cadre d'activités de surveillance ne peut avoir lieu que dans le cadre de garanties appropriées définies par la loi, conformément à l'article 8 de la Charte européenne des droits fondamentaux. Parmi ces garanties, figure l'exigence d'un contrôle indépendant et effectif, auquel les autorités de protection des données doivent être associées selon leurs compétences. »

Celui-ci recommande le contrôle par des autorités de protection des données indépendantes

afin d'éviter tout abus, selon leurs domaines de compétences, si une telle surveillance devait être mise en place. En France, la CNIL n'a encore jamais été commissionnée afin de faire un tel contrôle.

Il ne s'agit là que de quelques textes afin de démontrer la complexité juridique en la matière. De nombreuses législations et déclarations existent, à différents niveaux, apportant des ajustements… Mais rares sont les lois allant à l'encontre du droit à la vie privée. Ces lois sont généralement perçues comme allant à l'encontre d'une liberté fondamentale, et donc antidémocratique. Malheureusement, il en existe.

« Déclaration universelle des droits de l'homme », site Internet un.org, Nations Unies.

« Convention européenne des droits de l'homme », site Internet echr.coe.int, Cour européenne des droits de l'homme.

« Charte des droits fondamentaux de l'Union européenne », site Internet europarl.europa.eu, Parlement européen.

« Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29 », site Internet cnil.fr, Commission nationale de l'informatique et des libertés.

2.7 Actualités internationales

En 2013, Edward SNOWDEN a exposé une face cachée du gouvernement américain. Suite à ses missions successives aux seins de la NSA et de la CIA, il a rendu public plusieurs milliers de documents confidentiels nous laissant entrevoir un système de collecte des informations numériques organisé, à l'échelle mondiale. La majorité de ces systèmes ne ciblait pas les données qu'ils récoltaient. Ennemi ou allié, personne n'était à l'abri. Plusieurs dirigeants Européens ont ainsi été surveillés pendant plusieurs années.

PRISM, XKeyscore, Bullrun… font, entre autres, partie de la liste : PRISM pour récupérer le renseignement à la source (Facebook, Google, Microsoft, Apple, IBM, Cisco…), XKeyscore pour accéder à ces informations, Bullrun pour casser les technologies de chiffrement les plus vulnérables.

Suite à ces révélations, le gouvernement américain a démenti exercer une surveillance de masse. Le président Barak Obama s'était engagé à faire cesser ces agissements s'il s'avérait qu'ils existaient. Il est cependant difficile à évaluer si des mesures ont été prises.

Suite à ces révélations, Edward SNOWDEN s'est exposé aux sanctions américaines concernant la trahison. Il vit depuis en exil, sous couvert de l'asile politique russe.

« Revelations », site Internet edwardsnowden.com, Edward SNOWDEN.

« Edward Snowden: how the spy story of the age leaked out », site Internet theguardian.com, The Guardian.

« Edward Snowden Fast Facts », site Internet edition.cnn.com, CNN.

« Profile: Edward Snowden », site Internet bbc.com, BBC.

« Inner workings of a top-secret spy program », site Internet apps.washingtonpost.com, The Washington Post.

« NSA Prism program taps in to user data of Apple, Google and others », site Internet theguardian.com, The Guardian.

« XKeyscore : NSA's Google for the World's Private Communications », site Internet theintercept.com, The Intercept.

« Synthèse du programme de surveillance américain », site Internet linuxfr.org, LinuxFr.

2.8 Actualités nationales

Suite aux récents événements qui se sont produits en France, de nombreuses personnes montrent du doigt les moyens de télécommunication numérique qui sont à la disposition de personnes malveillantes.

2.8.1 France : Loi relative au renseignement

Suite aux multiples vagues d'attentats qui ont touché la France en 2015/2016, une proposition de loi a été faite, concernant la collecte d'informations par les services de renseignements.

Elle légalise la mise en place de « boite noire » (fonctionnant sur le principe du « Deep Packet Inspection », alias DPI) chez les fournisseurs d'accès Internet, afin de recueillir des informations de connexion de la quasi-totalité des lignes ADSL en France.

Elle stipule également qu'un algorithme sera mis en place afin de détecter toutes menaces potentielles, tout en préservant l'anonymat de la personne concernée, jusqu'au feu vert d'une autorité compétente. Cet algorithme pourrait se baser sur des informations de connexion, comme l'heure et l'adresse du site concerné, les adresses IP de source et de destination, l'utilisation de Tor ou tout autre moyen d'anonymisation…

Seul petit point noir au tableau, de nombreux sites sont passés au chiffrement total de leurs communications avec les utilisateurs (Google, Facebook, Twitter…) et nombre d'entre eux exploitent leurs centres de données hors du territoire Français.

2.8.2 Contourner le chiffrement des communications

En août 2016, Bernard CAZENEUVE a décrété vouloir lancer « une initiative européenne » contre le chiffrement, afin de faciliter l'interception des données.

Deux pistes :

- Interdire purement et simplement le chiffrement. Pas sûr que les acteurs majeurs (américains par exemple) acceptent de bon cœur.
- Obliger les différents services présents sur le Net à fournir les clés de déchiffrement pour permettre au gouvernement de surveiller leurs communications malgré les technologies de chiffrement employées. Idem, les entreprises étrangères risquent de faire de la résistance.

L'ANSSI (« Agence nationale de la sécurité des systèmes d'information ») a rapidement réagi en soulevant les problématiques de sécurité qu'une potentielle porte dérobée gouvernementale pourrait engendrer, aussi bien pour les particuliers que pour les entreprises. À l'heure du tout numérique (informations sur la vie privée, démarches administratives, banques en ligne…), de telles actions sont difficilement imaginables.

Dans le deuxième cas, nous parlons de séquestre des clés. Certains gouvernements ont mené des expérimentations sur le sujet : les États-Unis par exemple. La perte de la clé de chiffrement/déchiffrement peut être catastrophique pour un utilisateur ou une société. Avec les moyens de chiffrement actuels, il est impossible de récupérer les informations chiffrées sans la clé de chiffrement. Une entreprise qui aurait chiffré des informations sensibles et vitales à l'exploitation de son marché pourrait se voir mettre la clé sous la porte. Il est donc courant de conserver une copie de la clé de chiffrement en lieu sûr. Pour les petites organisations qui n'ont pas les moyens de le faire en interne sur un autre site géographique, il est possible de le faire via un tiers de confiance. Un notaire par exemple, qui ne remettra cette clé de chiffrement qu'à certaines personnes et si la situation remplit un certain nombre de conditions. Le gouvernement

américain était donc parti de ce principe : stocker et assurer la sécurité de ces clés de chiffrement gratuitement, proposant ce service aux particuliers comme aux entreprises. Rien d'obligatoire, sauf pour les entreprises travaillant avec eux, qui devaient se soumettre à ces exigences.

De telles pratiques peuvent être dangereuses si elles deviennent obligatoires. En effet, un gouvernement en possession de toutes les clés de chiffrements des citoyens et des entreprises qui résident sur son territoire n'aurait aucun mal à déchiffrer toutes les données sur lesquelles il pourrait mettre la main. Pour les particuliers, une atteinte grave au droit à la vie privée ; pour les entreprises, d'éventuelles concurrences déloyales et des risques d'espionnage industriel.

Si ceci venait à se réaliser, les propos des ONG tels que « Freedom House » ou encore « Reporters sans frontières » seraient d'autant plus vrais !

« LOI n° 2015-912 du 24 juillet 2015 relative au renseignement », site Internet legifrance.gouv.fr, Legifrance.
« Projet de loi relatif au renseignement », site Internet assemblee-nationale.fr, Assemblée Nationale.
« Loi relative au renseignement », site Internet senat.fr, Sénat.
« Loi Renseignement », site Internet wiki.laquadrature.net, la Quadrature du Net.

« Le point de vue d'OVH.com sur la loi renseignement », site Internet ovh.com, OVH.
« Projet de loi Renseignement », site Internet sous-surveillance.fr, Sous-Surveillance/la Quadrature du Net.

« Facebook follows Google with tough encryption standrad », site Internet theverge.com, The Verge.

« Bernard Cazeneuve veut « une initiative européenne » contre le chiffrement », site Internet lemonde.fr, Le Monde.

« Contre le chiffrement, le dangereux projet de Cazeneuve », site Internet lepoint.fr, Le Point.

« La Cnil et le Conseil national du numérique défendent le chiffrement des communications », site Internet lefigaro.fr, Le Figaro.

« Tristan Nitot : "Restreindre le chiffrement affaiblirait la démocratie" », site Internet franceinter.fr, France Inter.

« Contrôler le chiffrement : un calcul difficile pour le gouvernement », site Internet liberation.fr, Libération.

« surveillance://: Les libertés au défi du numérique : comprendre et agir », livre de Tristan Nitot, aux éditions C&F Éditions, 2016.

« Histoire des codes secrets », livre de Simon SINGH, éditions Le livre de poche, 2001.

2.9 Le facteur de l'ignorance

Tous les propos tenus précédemment dans ce document s'appuient sur des faits connus. Mais quand est-il de l'inconnu ?

Dans la partie « Théorie » sur la protection des données et l'anonymisation de cet état de l'art, nous avons vu les grandes étapes de l'évolution du chiffrement. Place à une note d'histoire.

2.9.1 Marie STUART

Marie STUART, souvent évoquée sous le nom de « Marie reine d'Écosse », fut victime de son ignorance. Elle fut envoyée en France et mariée à François IIe du nom afin de tisser une alliance. Pendant ce temps-là, sa cousine, la reine Élisabeth Ier monta sur le trône d'Angleterre, menant les conflits entre catholiques et protestant à leur apogée. À son retour en écosse, Marie fut arrêtée et mise en détention par Élisabeth sur les conseils de son « maitre-espion », Sir Francis WALSINGHAM, qui soupçonnait une conspiration pour la renverser. Pendant la détention de Marie, un catholique du nom de Gilbert GIFFORD prit contact avec l'ambassade de France à Londres, proposant de lui faire parvenir clandestinement du courrier. L'ambassade s'empressa d'accepter, voyant là un bon moyen de reprendre contact avec sa reine. Rapidement un groupe de sympathisants à la situation de Marie, prirent contact avec elle par ce biais. Il était question de la faire évader ainsi que de fomenter un coup d'État. Ils n'hésitèrent pas un instant à échanger ce genre d'informations compromettantes, ayant l'illusion d'une sécurité absolue amenée par le chiffrement de leurs messages. Malheureusement pour eux, ils ne se doutaient pas que GIFFORD travaillait pour Sir WALSINGHAM. Tous les messages, dans un sens comme dans l'autre, transitaient par son cabinet noir, où les sceaux étaient délicatement décollés à la vapeur, les lettres recopiées et réexpédiées une fois les sceaux recollés. Ni vu ni connu, il avait une copie avec laquelle il pouvait travailler au cassage du chiffrement. Une fois ce chiffrement cassé, il poussa le vice jusqu'à ajouter un post-scriptum en bas d'une des lettres de Marie,

demandant de lui faire connaitre les noms et les qualités des gentilshommes qui risquaient leurs vies pour elle, afin de les récompenser à leur juste valeur une fois le plan réalisé. Quelle ironie ! Les sympathisants de Marie n'hésitèrent pas un instant à répondre à cette requête, pensant encore une fois leur chiffrement inviolé. Il ne fallait pas plus de preuves à Sir WALSINGHAM pour convaincre la reine Élisabeth de faire exécuter sa cousine. Elle fut décapitée le 8 février 1587 au château de Fotheringhay. Malheureusement, les chroniques historiques font état ce jour-là de l'état d'ébriété du bourreau, qui dut s'y reprendre à 3 fois avec sa hache pour achever sa triste besogne, et fit tomber la tête par terre quand il la saisit pour la présenter au public rassemblé pour assister à l'exécution, n'ayant pas pensé que la perruque n'était peut-être pas assez solidement attachée.

2.9.2 1re guerre mondiale

En 1917, l'Allemagne prit conscience que le temps lui était compté si elle voulait remporter cette guerre. Il fut décidé de mettre en place un blocus total autour de l'Angleterre afin de couper tous les échanges commerciaux, le but étant de les affamer et de les pousser à capituler. Les dirigeants allemands avaient conscience qu'ils risquaient de faire voler en éclat la position de neutralité dans ce conflit, qui avait été adoptée par les États-Unis. Ils ont donc décidé d'envoyer un télégramme à l'ambassade d'Allemagne à Washington, pour qu'il soit ensuite transmis à Mexico. Ils proposaient aux mexicains d'attaquer les États-Unis afin de récupérer d'anciens territoires (Texas, nouveau Mexique et l'Arizona) avec leur appui. Ceci permettrait d'occuper les Américains le temps de faire capituler les Anglais. Malheureusement, le câble transatlantique le plus direct entre l'Allemagne et les États-Unis fut sectionné peu de temps avant. Le télégramme dut passer par la Suède et l'Angleterre avant de rejoindre sa première étape. Deux personnes du Bureau 40 s'attaquaient à décrypter ce message. La plupart des chiffrements utilisés au début du XXe siècle n'étaient que des évolutions de chiffrements déjà décryptés par le passé. Ils en vinrent rapidement à bout. La décision fut prise de ne pas le transmettre aux Américains directement, ceci aurait certes rempli l'objectif de les faire rentrer en guerre, mais aurait également révélé aux Allemands que leur chiffrement utilisé pour les

échanges diplomatiques et militaires était compromis. Il fut alors décidé de modifier le message intercepté avant de le rendre public dans les journaux. Les instructions destinées à l'ambassadeur allemand à Washington supprimées et l'adresse modifiée. Le courrier publié pouvait ainsi faire croire à une fuite d'informations du côté du gouvernement mexicain. Le 2 avril 1917, Wilson WOODROW, 28e président des États-Unis d'Amérique changea d'avis et encouragea le congrès à voter en faveur d'une implication directe dans cette guerre, afin de répondre aux encouragements hostiles des Allemands. Le secret sur l'interception des communications allemandes par les services de renseignement des Britanniques resta confidentiel. Il faudra attendre les années 20 pour qu'ils changent leurs méthodes de chiffrement.

2.9.3 Enigma

Suite aux découvertes d'Allan TURING et de son équipe à Bletchley Park, toute une stratégie fut mise en place afin de conserver le secret. En effet, contrer systématiquement les attaques allemandes aurait paru suspect et Enigma n'aurait pas tardé à évoluer (ajout de rotor, multiplication des câblages…), réduisant ainsi à néant tous les efforts et les sacrifices qui ont été faits jusque-là. La complexification du chiffrement aurait même pu priver les alliées de renseignements pour plusieurs décennies. Ceci aurait causé de nombreuses pertes civiles et militaires et peut-être même changé l'issue de cette guerre. Ainsi, une fois l'information déchiffrée, il fallait décider s'il fallait intervenir ou non. Les personnes qui ont dû prendre ces décisions devaient passer outre la morale. Il était parfois nécessaire de laisser des centaines d'innocents périr sans bouger. Si la décision d'intervenir était prise, il fallait s'arranger pour faire parvenir aux oreilles des Allemands qu'ils avaient été déjoués par d'autres moyens : faire survoler un avion quelques minutes avant un bombardement, émettre de fausses communications radio non chiffrées…

Ces trois courts exemples ne peuvent pas à eux seuls faire prendre conscience aux lecteurs de ce document l'étendue de l'importance du facteur d'ignorance au travers de l'histoire. Les

exemples se comptent par centaines et peut-être même plus si nous appliquons ce fameux facteur ici même. L'Angleterre a mis plusieurs décennies avant de déclassifier les informations sur Enigma.

Ainsi, toutes les informations connues concernant les méthodes de chiffrements et d'anonymisation modernes considérées comme fiables sont peut-être toutes ou en partie compromises sans que nous le sachions. Nous croyant en sécurité en utilisant ces technologies, nous perdons de vue la possibilité d'une potentielle interception ou d'une utilisation malveillante d'un groupe indépendant ou d'un gouvernement.

Mais ça, nous ne le savons pas, nous ne pouvons qu'émettre des suppositions…

« Histoire des codes secrets », livre de Simon SINGH, éditions Le livre de poche, 2001.

« Cryptologie : art ou science du secret ? », site Internet ssi.gouv.fr, ANSSI.

3. Études terrain

3.1 Interviews

3.1.1 Méthodologie

Les personnes interviewées ont été choisies en fonction de plusieurs critères :

1. Chaque personne devait être représentative d'une portion de la population : une personne parlant en tant qu'utilisatrice, une personne ayant une vision inter entreprise et une personne ayant une forte expérience dans le domaine de la sécurité des systèmes d'information et des télécommunications.

2. Les personnes choisies devaient avoir une connaissance minimale des outils numériques (réseaux sociaux, moteur de recherche…) ainsi qu'un sens critique et une argumentation solide afin d'imager leurs opinions.

3. Il devait être possible d'organiser une rencontre en face à face ou une téléconférence dans le pire des cas, afin de permettre un échange le plus naturel possible et le plus fluide possible.

Les interviews ne devaient pas dépasser une heure afin de ne pas monopoliser le temps des personnes qui ont eu la gentillesse de m'accorder ces interviews. Cela permettait aussi de faciliter la synthétisation des propos échangés.

Les échanges ont été enregistrés à l'aide d'un dictaphone, afin de ne pas perdre de temps en prise de notes sur le moment, de faciliter le dialogue et d'avoir un support ne pouvant pas altérer le sens des propos tenus.

L'interview était guidée par une liste de questions afin de suivre le fil directeur de la

problématique de cette thèse professionnelle. L'ordre des questions était susceptible de changer en fonction de la personne interviewée et des réponses aux questions précédentes. La formulation de celles-ci pouvait également varier. De cette façon, la personne interviewée était libre d'imager ces propos, de rebondir sur un autre sujet…

Une fois les résumés des interviews retranscrits par écrit, les personnes interviewées les ont relues, en bénéficiant d'un droit de modification, avant de donner leur accord final pour utilisation dans ce document.

3.1.2 Présentation des personnes interviewées

Christophe BRAND

Il est PDG de la société Datadvance, joint-venture d'Airbus Group depuis les années 2000. Il représente la partie grand public de la population. Il n'a pas d'expérience notable dans le domaine de l'informatique, mais en a une utilisation et une connaissance tout à fait honorable.

Bertrand DESPREZ

Il occupe le poste de responsable au sein d'un service informatique d'Airbus Group. Il a une connaissance approfondie de la mise en place et de l'utilisation de l'informatique dans le milieu professionnel.

Pierre-Yves PARIS

Il possède un CV très fourni dans le domaine de la sécurité informatique. Il est actuellement consultant senior en sécurité des systèmes d'information pour le compte de la société Sogeti. Il possède également une connaissance poussée de l'utilisation des réseaux sociaux et de leurs fonctionnements.

3.1.3 Retours et analyse

3.1.3.1 Efficacité et pertinence de la surveillance de masse

Les trois personnes interviewées sont quasiment convaincues de l'efficacité de la surveillance de masse. Je ne parle pas de résultats finaux, mais de capacité à recueillir, stocker et analyser les informations.

Recueillir des informations, pour cela il y a les fameuses « boites noires » qui sont installées dans toutes les infrastructures des fournisseurs d'accès à Internet, datacenters… en France. À l'international, il est peu probable que tous les gouvernements aient ces moyens à leur disposition. Ceci nécessite des ressources importantes ainsi qu'une réelle volonté de recueillir des renseignements sur chaque individu. Pour en arriver là, il faut qu'il existe un certain climat émotionnel. En France, les événements récents, relayés par les médias en sont un très bon exemple. Il serait très difficile de faire adopter de telles mesures en temps de paix dans une démocratie. Nous savons tout de même que les États-Unis en font usage. Les révélations d' Edward SNOWDEN sur les programmes de surveillance de la NSA ont permis d'avoir un aperçu de leurs ampleurs. Non contents de le faire sur leur territoire, ils se permettent également de le faire à travers le monde entier, allant jusqu'à surveiller des chefs d'État alliés. Pour en arriver à une telle échelle, ils ont recours aux grands acteurs du Net, qui sont majoritairement implantés outre Atlantique. Collaboration, pression, infiltration… Tous les moyens sont bons. Donc oui, recueillir des informations sur l'utilisation des moyens numériques de l'intégralité des individus résidant dans un pays est tout à fait de l'ordre du possible.

Concernant le stockage, ceci doit représenter une masse importante d'informations. Mais rien d'infaisable. N'oublions pas qu'il s'agit là d'un projet mené par un gouvernement, et qui plus est, à des fins de recueil de renseignements. Les informations ont une valeur importante, surtout pour un gouvernement. De plus, les progrès technologiques au cours des dernières décennies vont dans ce sens. Chaque année le prix du stockage des données numériques diminue tandis que la densité de stockage augmente. Là où, il y a dix ans, ceci aurait été difficilement imaginable, cela l'est aujourd'hui. Il faut également prendre en compte le fait que

la consommation de contenus numériques est en hausse constante. En France, la loi relative au renseignement fait seulement état de recueil des métadonnées, donc si la consultation de contenus numériques via Internet augmente, le stockage des renseignements aussi, mais pas de façon similaire.

Pour l'analyse des données… Comme en fait mention Christophe au cours de son interview, le service des impôts français fait usage du traitement de masse des informations et ils le font de façon relativement efficace. Nous sommes aujourd'hui dans un monde de plus en plus dépendant du Big Data. Derrière ce nom barbare se cache une discipline qui peut être décrite d'une façon simplifiée par l'analyse de résultat provenant de croisements et d'associations d'informations n'ayant pas forcément de liens directs entre eux. Les supermarchés utilisent le Big Data avec nos cartes de fidélités, les banques, l'industrie… L'efficacité de telles méthodes sur des métadonnées de connexion Internet ne fait aucun doute. À partir des sites que l'on visite, la durée passée sur ceux-ci, la récurrence de leurs consultations… Il devient évident qu'il est possible de dresser le profil d'un utilisateur : radicalisation d'un individu, orientation religieuse, opinions politiques, orientation sexuelle…

Pertinence de la surveillance de masse… deux choses : l'efficacité réelle et les dérives possibles.

Aujourd'hui il existe de nombreux moyens de sécurisation et d'anonymisation du trafic des données transitant sur Internet. Ces moyens sont couramment utilisés par les entreprises afin de garantir la confidentialité de leurs échanges numériques pouvant impacter leurs revenues économiques (contrats, innovations…), mais ils le sont également par des particuliers.
La loi HADOPI qui a été adoptée par la France en 2009 en est un exemple. Cette loi a pour but de lutter contre les téléchargements illégaux d'œuvres numériques. Une rapide recherche sur Internet nous indique comment la contourner. VPN, Tor… les moyens ne manquent pas. Un particulier peut souscrire à un abonnement à un service de VPN pour environ 5€ par mois (voir moins) en quelques clics. Son trafic sera chiffré et il aura la possibilité de ressortir au grand jour sur Internet depuis un autre pays, n'ayant pas ce genre de législation. Les personnes qui

recevront un email d'avertissement en cas de transgression de cette loi, seront en majorité des personnes non informés et ne faisant un usage que très occasionnel du téléchargement illégal. Pendant ce temps-là, les plus gros consommateurs d'œuvres numériques diffusées par des moyens illégaux, qui eux sont informés, peuvent dormir sur leurs deux oreilles.

Il en va probablement de même avec le renseignement de masse tel qu'il est utilisé en France. Les personnes mal intentionnées prendront majoritairement des précautions. Être un criminel au XXIe siècle sans avoir une connaissance minimale dans les technologies du numérique entraine dans une forte majorité des cas une fin de carrière prématurée. Des groupes terroristes tels que l'État islamique ou Al-Qaïda sont suffisamment importants et probablement suffisamment organisés pour avoir pensé à ce genre de risques. Ben LADEN a fait partie pendant plusieurs années de la CIA. Partant de ces faits, nous pouvons donc en déduire que la quasi-totalité du trafic analysé par les services de renseignements français est « inoffensif ». La partie restante se compose en grande majorité de criminels de bas étage ne prenant pas ce genre de précaution et d'une minorité d'informations pertinentes dues à une erreur humaine (oubli d'utilisation de protocoles…), une erreur technique (déconnexion du VPN…)… Comme évoqué, il serait tout de même possible d'analyser les métadonnées en recherchant des traces de tentatives de chiffrement et d'anonymisation. Mais au vu de l'étendue de leurs utilisations, il serait compliqué de déduire si le comportement d'un internaute est suspect ou non.

Sauf si… comme évoqué dans l'état de l'art, le facteur d'ignorance n'est pas à négliger. Nous savons que l'utilisation de technologies de chiffrements et d'anonymisation n'est pas une garantie absolue. En effet, ces technologies dépendent directement de la méthode de chiffrement adopté, la longueur des clés… Un certain nombre de technologies est connue pour être vulnérable, en particulier aux services de la NSA. Mais les autres, celles que nous pensons inviolables, le sont-elles réellement et si oui, pour combien de temps ? Le saurons-nous rapidement le jour où elles seront compromises ? Comme nous le montre l'histoire, l'ignorance qu'une technologie de chiffrement a été compromise est un enjeu capital dans le domaine du renseignement.

Le recueil des informations : possible. Le stockage : possible. L'analyse : possible. La

pertinence… Tout dépend si les technologies de chiffrement et d'anonymisation modernes sont efficaces. Si elles le sont, les moyens et les ressources que la surveillance de masse exige sont colossaux comparés aux résultats qu'elle apporte. Dans ce cas-là, il faudrait se poser la question si la justification de son utilisation est vraiment celle qui nous est présentée c'est-à-dire un enjeu sécuritaire, ou bien autre chose : contrôle de la population, fichages… En revanche, même si les technologies modernes de chiffrement et d'anonymisation sont obsolètes et que cette information n'est pas rendue publique, elle peut être extrêmement efficace, même contre des groupes organisés.

Dans les deux cas, ceci doit être encadré et contrôlé de très près. Les exemples de dérives de mauvaise utilisation sont multiples. L'utilisation de telles méthodes est rarement compatible avec la notion de démocratie. La quasi-totalité des pays utilisant ce genre de méthodes sont des régimes totalitaires : Corée du Nord, Érythrée, Arabie Saoudite… La liste est longue. Les exemples dans l'histoire sont également nombreux. Pour n'en citer qu'un, la montée du Nazisme en Allemagne dans les années 30. La Gestapo fut chargée de ficher tous les juifs, les homosexuels… La suite est tristement connue. Imaginez que l'histoire se reproduise aujourd'hui, avec les moyens technologiques qui existent. En 2017, nous élirons notre futur(e) président(e) de la République. Nous ne pouvons pas anticiper qui sera élu et quelle utilisation il/elle fera de ce système de collecte d'informations de masse. Nous ne savons pas quels évènements peuvent survenir dans 10, 20, 30 ans… et quelles conséquences cela peut avoir sur la démocratie en France. L'histoire nous le démontre encore, la paix n'est malheureusement jamais sans fin. Elle peut durer des siècles, mais tôt ou tard, il y aura une période de crise/conflit.

3.1.3.2 Vie privée et Internet

Ces interviews ont mis en évidence que la frontière entre la vie privée et l'utilisation d'Internet est très mince. Internet faisant de plus en plus partie intégrante du quotidien, nous ne nous rendons pas forcément compte de l'ampleur du phénomène.

Il y a d'un côté les informations que nous transmettons de notre plein gré (réseaux sociaux…), et d'un autre les informations que les différents services que nous utilisons récupèrent sur nous.

La première partie est contrôlable. C'est à chacun de se fixer des limites sur ce qu'il accepte d'exposer à propos de sa vie privée et les conséquences que cela peut entrainer. Les réseaux sociaux développent parfois chez certains individus une sorte de dépendance, biaisant la perception de ces limites.

La deuxième est plus difficilement décelable. En effet, ces services ne nous demandent pas systématiquement la permission de récupérer et d'exploiter certaines informations. Google, par exemple, récupère par défaut tous vos historiques de localisation, de vos recherches… Lors de l'inscription à ses services en ligne (Gmail, Google+…), il vous oblige à cocher une case, certifiant que vous avez lu et que vous acceptez les « conditions générales d'utilisation » (CGU) de ces services. Le lien vers celles-ci se trouve à côté de cette case à cocher. Malheureusement, malgré toute la bonne volonté de l'utilisateur, peu de personnes les lisent de bout en bout. Ces conditions générales d'utilisation sont souvent rédigées dans un jargon juridique et technique complexe. Face à un tel document, l'utilisateur lambda est souvent découragé, il coche la fameuse case et clique sur « continuer ». Ces CGU sont également amenées à évoluer régulièrement. Ceci n'est qu'un exemple parmi tant d'autres. Tous les services en ligne font usage de ce genre de pratiques.

Toutes ces données ainsi récoltées (volontairement fournies par l'utilisateur ou à son insu) sont couramment utilisées à des fins de profilage. Comme expliqué précédemment, le Big Data permet de recouper de nombreuses informations entre elles afin de faire ressortir certains résultats. Un exemple des plus marquant concernant le profilage est la publicité ciblée. Vous avez probablement constaté suite à la visite d'un site e-commerce concernant un achat potentiel, l'apparition de publicités concernant l'objet en question (ou une déclinaison) alors que vous naviguez sur des sites qui n'ont aucun rapport. Ceci peut également subvenir suite à

un échange d'emails où vous auriez manifesté votre intérêt pour cet article. Le but premier d'une entreprise est de faire des profits. Pour faire des profits, il faut vendre des articles ou des services. Si un utilisateur reçoit de la publicité pertinente, en fonction des sites qu'il a visités ou des informations qu'il a transmises, il y a de fortes chances pour qu'il clique dessus, rapportant ainsi de l'argent par son clic à la régie publicitaire (la société qui se charge de proposer la publicité) ainsi qu'à l'entreprise à laquelle il va acheter cet article. Cet usage de nos données personnelles reste dans le domaine de l'acceptable… comparé à la suite.

Les géants qui dirigent Internet sont souvent plus riches que la plupart des états et hors d'atteinte de nos lois. Google a été condamné par la CNIL à 100 000€ d'amende en 2016, concernant le non-respect du droit au déréférencement par leur moteur de recherche. Que représente 100 000€ pour Google ? Le salaire moyen annuel d'un employé. Google dépense chaque année 80 millions d'euros pour nourrir ses employés. Autant dire, une miette de pain. Ces entreprises sont également souvent implantées aux États-Unis, compliquant d'autant plus les démarches administratives en cas de recours individuel ou collectif d'utilisateurs mécontents ne résidant pas là-bas.

Google récolte des tas d'informations sur vous, vos habitudes et votre entourage. Certaines études mettent en évidence qu'une entreprise comme Google vous connaît mieux que vos parents, votre conjoint(e), voire même que vous-même ! À côté de ça, Google investit des milliards et mène des recherches en robotique militaire, aérospatiale, intelligence artificielle, immortalité (oui, vous avez bien lu)… On sent venir la suite, digne d'un film de science-fiction des années 60.

Mark ZUCKERBERG, fondateur de Facebook, a déclaré que la notion de vie privée avait évolué. En effet, nous le constatons, même si de nombreuses données sur nous ne sont pas publiées au grand jour sur Internet, elles sont utilisées à d'autres fins, souvent à notre insu. D'autres peuvent être publiées à notre insu, par des proches, des journalistes… Sans avoir un contrôle direct dessus. De plus, souvent, elles ne nous appartiennent plus entièrement. Facebook stipule

dans ses conditions générales d'utilisation qu'il peut les utiliser à des fins commerciales, les transmettre à des tiers, les revendre... Elles échappent ainsi à notre contrôle.

3.1.3.3 Législations

Comme évoqué précédemment, Internet représente la mondialisation de l'information et l'instantanéité de sa diffusion. Face à ça, chaque pays possède sa propre législation. De nombreuses incohérences existent entre elles. Si quelque chose est déclaré illégal dans un pays, il suffit d'utiliser une méthode d'anonymisation pour le faire dans un autre, en évitant quasiment tout risque de poursuite judiciaire.

Partant de ce constat, il serait logique de vouloir harmoniser les législations. Un organisme indépendant, chargé de ceci ainsi que de son application, à l'image de « l'Organisation des Nations unies » (avec l'efficacité en plus), pourrait être une solution. Malheureusement quatre difficultés majeures existent.

Tout d'abord, cette entité doit être neutre et impartiale : simple à énoncer, mais très complexe à réaliser. Comment empêcher les états et les géants du Net, avec leurs ressources financières titanesques, de ne pas travailler dans ce sens ? Soudoyer des membres de cette organisation, les intimider, ou encore les infiltrer.

L'efficacité. Comment veiller au respect des législations mises en place ? Quelles sanctions peuvent être adoptées ? Il faut qu'elles puissent être dissuasives même pour les entités les plus importantes, mais également réalistes pour les plus petites et les particuliers. Comment les obliger à s'y soumettre ?

Troisième point : comment faire en sorte que tous les pays adhèrent à cette organisation ? Si un seul pays reste en marge de celle-ci et que ses lois sont permissives ou inexistantes sur de nombreux sujets, le système est faillible.

Enfin, la différence des cultures : il s'agit probablement de la plus grosse difficulté à surmonter. Ce qui peut paraitre acceptable pour les uns ne le sera pas forcément pour les autres. Plusieurs exemples peuvent être pris pour démontrer la difficulté de la tâche : l'achat de certains articles en ligne est légal dans certains pays et illégal dans d'autres ; la protection des droits d'auteur ; la qualification des contenus (maltraitance animale, traite d'êtres humains, pédopornographie…). Et bien d'autres… Autant de sujets qui relèvent de la juridiction et de la culture propre à chaque pays. Une telle organisation serait éventuellement du domaine du possible si chaque état pouvait apporter des spécificités législatives, mais, par la même occasion, perdrait une grande partie de son intérêt.

Autant de difficultés complexes, voire impossibles à résoudre. Malgré l'idée de base qui pourrait être séduisante par de nombreux aspects, un organisme indépendant harmonisant les législations reste une utopie.

3.1.3.4 Le monde du logiciel Libre

J'ai principalement débattu de ce sujet avec Pierre-Yves. Il s'agit d'un sujet sortant du fil directeur que je m'étais initialement fixé, mais qui, je pense, a tout à fait sa place dans cette thèse.

Initialement, lorsqu'un utilisateur achetait l'un des tout premiers ordinateurs personnels, il était livré avec très peu de logiciels préinstallés. C'était à l'utilisateur de coder les logiciels dont il avait besoin. Il était fréquent de partager ses codes sources avec son entourage, qui pouvait alors le modifier à son tour pour coller à son utilisation, le redistribuer… Les utilisateurs avaient alors pleinement le contrôle sur leurs données.

Pour répandre l'informatique et son utilisation chez les professionnels et les particuliers, il était évident de devoir simplifier tout cela.

Rapidement, les grosses sociétés du marché de l'informatique commencèrent à fournir des outils clé en main, parfois même préinstallés sur leurs systèmes d'exploitation. Aujourd'hui, un ordinateur sorti de la boite nous propose une calculatrice, un outil de traitement de texte basique, un explorateur de fichiers… Cette pratique explosa avec l'avènement d'Internet, permettant une distribution simplifiée de logiciels. À des fins de portabilité et de simplification, le code source des logiciels était compilé (transformé d'un langage compréhensible par un être humain à un langage compréhensible par des machines) avant d'être distribué. L'utilisateur final perdit dans la majorité des cas la possibilité d'auditer ou de modifier les codes sources des logiciels qu'il utilisait.

Mais pas toujours ! En effet, le monde du logiciel Libre n'est pas mort.

Il est possible aujourd'hui d'installer un système d'exploitation entièrement libre de façon assez simple. GNU/Linux est l'un d'eux. Il en existe de nombreuses distributions différentes, grâce à l'accessibilité par tous du code source, permettant d'adapter ce dernier à une utilisation particulière. Certains sont plutôt orientés pour les serveurs, d'autres pour l'utilisation sur des ordinateurs personnels…

De nombreux logiciels libres existent également. Suites office (traitement de texte, tableur…), éditeurs d'images, navigateurs Internet…

Malheureusement, leurs utilisations restent anecdotiques (bien qu'en progression) face à l'offre des entreprises commerciales.

Les services proposés sur Internet sont également concernés. Il existe des réseaux sociaux libres, des services de stockage de fichiers libres, des services d'email libres…

Framasoft est une association française qui milite pour le monde du Libre. Elle met à

dispositions un grand nombre d'outils respectant ces valeurs. Il s'agit d'une belle démonstration qu'il est possible aujourd'hui de s'affranchir d'un grand nombre d'outils et de services en lignes utilisant leurs utilisateurs comme des produits.

Il reste cependant des domaines délicats et pas des moindres. Aujourd'hui un grand nombre de personnes possède un téléphone dit « intelligent » : les fameux smartphones. Bien qu'il y a eu des tentatives dans ce sens, aucunes ne sont vraiment abouties : Firefox OS, Ubuntu Touch… Il est difficile de se procurer un terminal sous ces systèmes, les spécifications matérielles sont souvent obsolètes, les applications disponibles ne sont pas légion… De nombreuses causes empêchent leurs apparitions massives. Pourtant le smartphone est probablement l'objet le plus irrespectueuse qu'il soit de la vie privée.

3.2 Sondages

3.2.1 Méthodologie

Le sondage a été réalisé afin que n'importe qui, sans connaissance particulière dans le domaine de la liberté de l'information, puisse y répondre en moins d'une minute. Il se compose de dix questions possédant chacune deux à trois réponses simples et directes.

Ce sondage a été réalisé sur un outil en ligne, permettant sa diffusion par Internet. 95 personnes y ont participé.

Il a été publié de plusieurs façons, plus ou moins performantes, mais en gardant à l'esprit de toucher un panel le plus large possible, touchant ainsi un maximum de milieu socioprofessionnel, culturel, de tranches d'âge…

3.2.2 Présentation des moyens de diffusion

1. **Réseaux sociaux**

   Twitter et Facebook ont été des sources non négligeables.

   Le sondage a été tweeté à des personnalités du Web et des associations concernées par ces problématiques, mais pas uniquement. Certains ont eu la gentillesse de retweeter, m'apportant une visibilité importante, et par conséquent des participations.

   Facebook y a également contribué. Publié sur mon mur et sur quelques groupes, un certain nombre de personnes a participé et parfois partagé mon post.

2. **Forum**

   Étant membre d'un forum concernant la pogonotomie, j'ai, sans trop d'illusions, partagé mon sondage avec les autres membres. Quelle n'a pas été ma surprise en constatant un

taux de participation qui dépassait mon imagination !

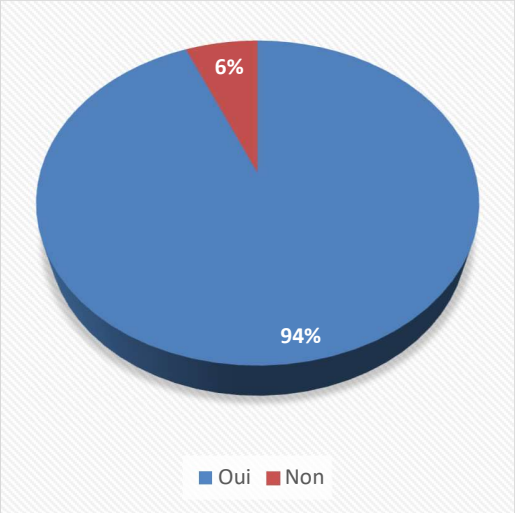
Ce forum est un lieu d'échange dans sa plus brève définition. La liberté d'expression en est la clé. De nombreux sujets y sont abordés autres que le sujet principal qu'il traite. La communauté est transgénérationnelle (de ~14 à 99+ ans), multiculturelle (Français, Belges, Suisses, Québécois…) et possède un fort panachage socioprofessionnel. Un sujet anodin peut vite donner le jour à des débats houleux, tout en gardant le respect et la bonne humeur en ligne de mire. Terrain parfait pour mon étude ! Les réactions et les commentaires ne se sont pas fait attendre.

3. **Emails**

Le sondage a été envoyé à plusieurs promotions du CESI via l'intermédiaire de mon responsable de formation, Olivier BUFFAT. Il a sélectionné en priorité des promotions n'ayant aucun rapport direct avec le milieu de l'informatique, afin de panacher le plus possible les réponses. C'est le moyen le plus classique, mais également celui qui est le moins efficace en terme de participation.

3.2.3 Résultats et analyse

Apportez-vous une valeur aux données numériques concernant votre vie privée ?



94% des personnes sondées accordent une valeur aux données relatives à leur vie privée, contre 6% qui n'y accordent aucune importance.

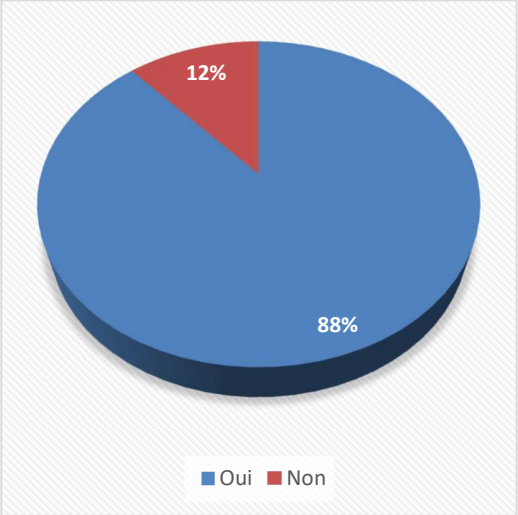
L'importance des réponses positives démontre qu'une majorité de personnes a conscience des enjeux que de telles données impliquent.

Les 6% de réponses négatives peuvent être en

partie dues au fait d'une banalisation de la notion de vie privée par les géants du Net et de l'avènement de l'hyper communication.

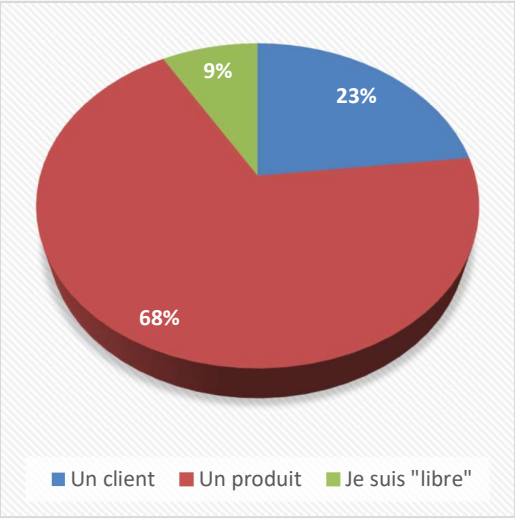
Utilisez-vous des objets connectés au quotidien (smartphone, smartwatch, tracker d'activité…) ?

88% admettent utiliser des objets connectés au quotidien, contre 12% qui revendiquent leur indépendance vis-à-vis de ces technologies.



Au vu du résultat à la question précédente, nous pouvons en déduire qu'une large majorité d'utilisateurs d'objets connectés le font en ayant conscience de l'utilisation potentielle de leurs données.

Quand vous utilisez des services tels que Google, Facebook… Pensez-vous être le client, ou bien le produit ?



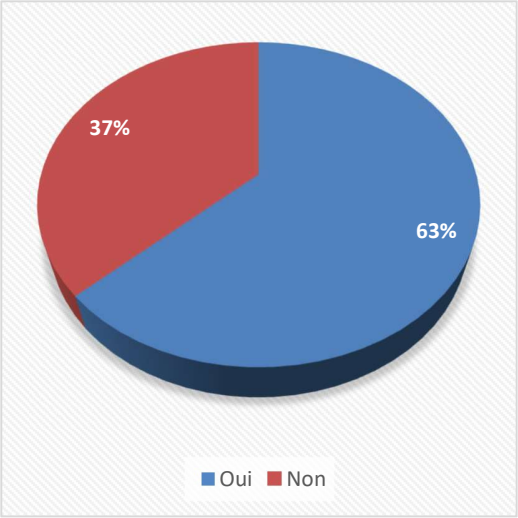
9% revendiquent être « libre ». Il est probable que ce pourcentage se retrouve dans les 12% de personnes qui ont reconnu ne pas utiliser d'objets connectés à la question précédente.

En revanche, dans les 88% reconnaissant utiliser au moins un objet connecté, une grosse partie des 23% pensent être en position de client. Nous pouvons en déduire qu'ils ne sont pas forcément en

connaissance des pratiques de l'exploitation à des fins commerciales de nos données par ces mêmes géants du Net qui produisent ces périphériques. Il est également possible qu'une petite partie de ces 23% ne voit pas d'inconvénient à l'utilisation de leurs données en échange des services proposés.

Suivez-vous régulièrement l'actualité concernant les nouvelles législations du « numérique » ?

63% admettent suivre régulièrement l'évolution des législations pouvant impacter l'utilisation du monde numérique, contre 37% qui prétendent ne pas le faire.

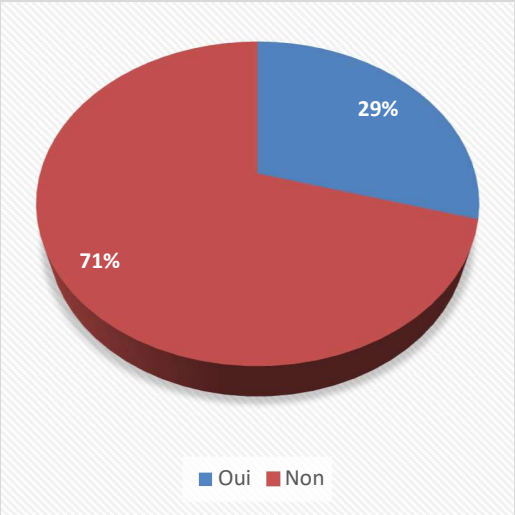


Les législations dans le domaine du numérique peuvent être grossièrement départagées en trois catégories : celles qui vont dans le sens de la protection de l'utilisateur, celles qui le réprimandent en cas d'infractions ou de délits et celles qui peuvent porter atteinte aux droits de l'utilisateur sous motif de servir des intérêts supérieurs.

Il semble primordial pour n'importe quel utilisateur du numérique d'effectuer une veille de ces trois catégories de législation : la première peut nous procurer des moyens pour nous défendre face à des pratiques douteuses. Si on ne connait pas nos droits, comment les faire respecter ? La deuxième, au même titre qu'un automobiliste surveille l'évolution du code de la route, un utilisateur du numérique doit savoir ce qu'il a le droit ou n'a pas le droit de faire. Comment faire pour rester dans la légalité si on n'est pas en connaissance des pratiques prohibées ? La dernière catégorie est un devoir de chaque citoyen : s'assurer que les lois adoptées par ses représentants ne vont pas à l'encontre de la définition d'une démocratie, sans justification valable. Si c'est le cas, il a le devoir de se faire entendre afin d'attirer l'attention sur ces dangers.

Il semblerait qu'il y ait encore du travail à faire auprès du grand public pour le sensibiliser à cette veille.

Considérez-vous la surveillance de masse et la censure d'Internet (loi renseignement…) comme étant compatibles avec une démocratie ?



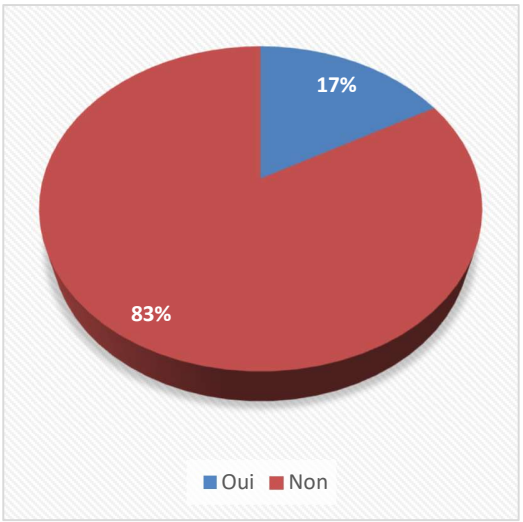
29% pensent que la surveillance de masse et la censure d'informations sont compatibles avec une démocratie, contre 71% qui pensent le contraire.

Dans une majorité des cas, un gouvernement qui impose ces pratiques à son peuple ne mérite pas la qualification de démocratie.

Mais des exceptions peuvent exister…

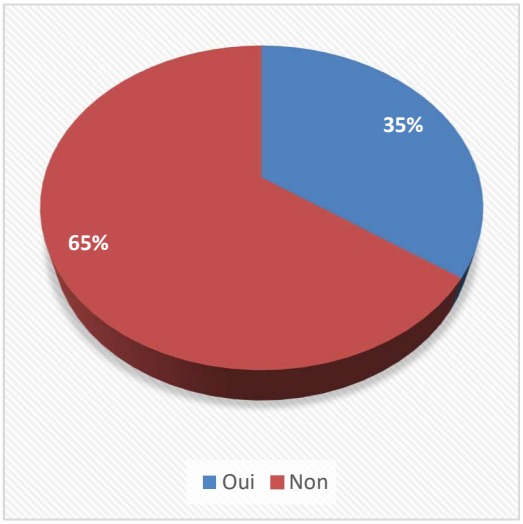
Pensez-vous que la surveillance de masse est pertinente/efficace ?

17% croient en l'efficacité et en la pertinence de la surveillance de masse, contre 83% qui n'y croient pas.



Les 29% des utilisateurs ayant répondu par l'affirmative à la question sur la compatibilité entre la surveillance de masse et la démocratie ont radicalement fondu de 12%. Ces 12% restant croient en cette compatibilité, mais pas en son efficacité ou en sa pertinence.

Êtes-vous prêt à sacrifier une partie de votre liberté au profit d'un motif sécuritaire potentiel ?

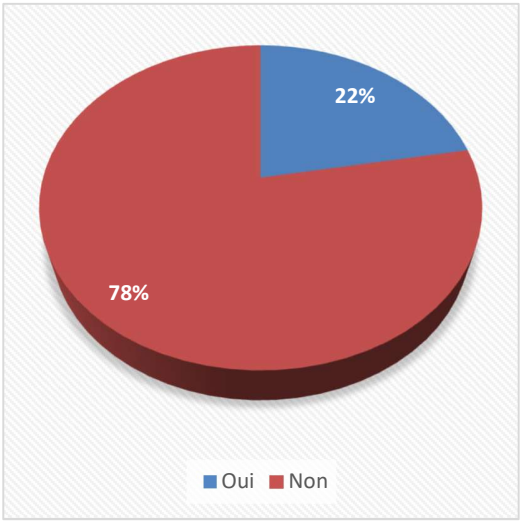


35% se sont déclarés favorable à sacrifier une partie de leur liberté au profit d'un motif sécuritaire, contre 65% d'avis défavorables.

Les réponses à cette question sont plus compliquées à analyser. En effet, il appartient à chacun de faire appel à son sens de la morale, et ainsi choisir entre la sécurité ou la liberté. Les deux ne s'excluent pas l'une de l'autre, divers niveaux de compromis peuvent être effectués.

Pensez-vous ne rien avoir à cacher à « Big Brother » ?

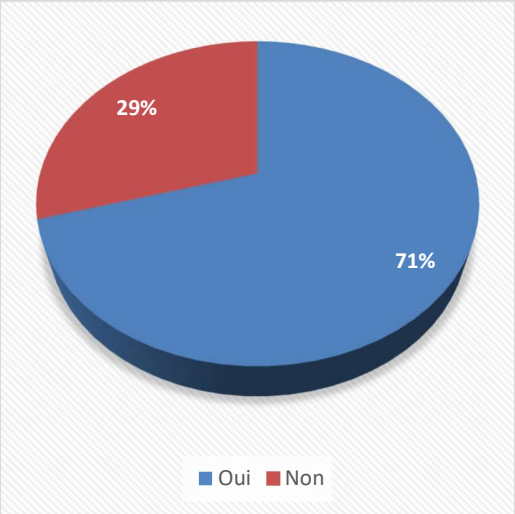
22% des personnes sondées pensent ne rien avoir à cacher à un potentiel programme de collecte de renseignements de masse, contre 78% qui pensent le contraire.



Là aussi, tout dépend de la notion de vie privée que chacun perçoit. Les 22% ayant répondu par l'affirmative peuvent avoir un degré de perception de la vie privée différent ou encore accepter que ce genre de données soit récupéré et analysé à des fins officielles. En revanche, les 78% ayant répondu par un avis négatif estiment probablement que ces données doivent rester en leurs possessions, et surtout sous leur contrôle.

Comme la question précédente, il s'agit vraiment d'un avis propre à chacun.

Avez-vous entendu parler de la notion de « neutralité du Net » ?

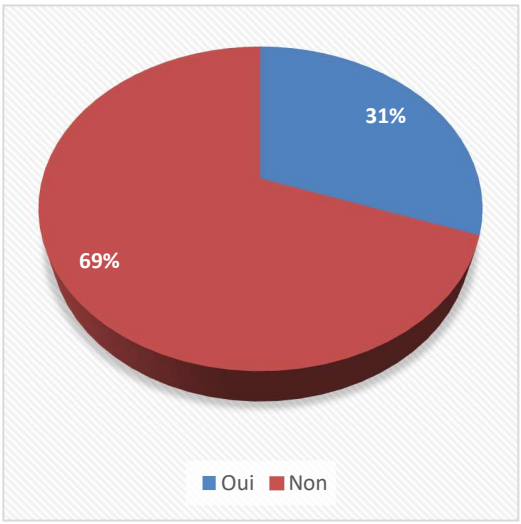


71% déclarent avoir déjà entendu parler de la notion de neutralité du Net, contre 29% qui ont répondu par la négative.

La notion de neutralité du Net met en avant les notions de liberté et de droits des internautes. Elle défend un Internet ouvert et l'égalité entre tous les Internautes.

Des associations comme la Quadrature du Net, Framasofts… se mobilisent pour sensibiliser le grand public à cette cause. Même si elles ont du mal à se faire entendre, 71% : c'est déjà une victoire en soi. Certains pays ont maintenant franchi le cap et ont inscrit la neutralité du Net dans leurs constitutions.

Pour vous, le fait que chaque pays possède sa propre législation concernant l'utilisation d'Internet vous semble-t-il cohérent avec la mondialisation de l'information qu'il offre ?



31% pensent qu'il est cohérent que chaque pays ait la liberté de définir sa propre législation concernant les usages du numérique, contre 69% qui pensent le contraire.

Comme abordé dans l'analyse des interviews, aucun des deux systèmes n'est parfait. Malgré les

faiblesses évidentes du système actuel, il a l'avantage d'être concret et non une utopie.

Au cours des réponses aux différentes questions, nous retrouvons des proportions de votes qui reviennent régulièrement. D'un côté les personnes sensibles à ces problématiques et de l'autre celles qui ne s'en préoccupent pas ou très peu. La deuxième partie de ces personnes peut s'expliquer de deux façons : les personnes n'ayant pas connaissance de l'utilisation abusive de leurs données personnelles, et celles qui en ont conscience, mais qui jugent le prix à payer acceptable face aux services ou à la sécurité que cela apporte.

Il s'agit d'une analyse personnelle des résultats, avec ma perception propre concernant de ces problématiques. Il est également possible que tout le monde n'ait pas la même compréhension des questions, ou encore que le caractère binaire des réponses proposées empêche la perception de différentes nuances.

4. Conclusion

4.1 Réponse à la problématique

La notion de vie privée est un droit fondamental. Ce droit comporte entre autres la maitrise de son partage avec autrui. La surveillance de masse et le profilage vont à l'encontre de cette notion. Ils s'appliquent sans l'approbation de l'utilisateur et sans qu'il puisse avoir connaissance ne serait-ce que des informations concernées.

Il est compréhensible qu'un gouvernement doive pouvoir recueillir des renseignements. En revanche, cela doit être fait en respectant le droit à la vie privée, pour quelques motifs que ce soit. Le fait de l'imposer à tous, sans restriction aucune, vient à l'encontre de ce dernier.

Le profilage peut apporter une plus-value à un service, mais pour qu'il respecte le droit à la vie privée, l'utilisateur doit pouvoir dire quelles informations il souhaite partager et quand. De même, l'utilisation de ces renseignements doit être faite uniquement dans le cadre initialement communiqué à l'utilisateur.

Partant de ces principes… La surveillance de masse pour quelques motifs que ce soit et le profilage ne sont pas compatibles avec la notion de vie privée.

4.2 Réponse aux hypothèses de travail

L'accès aux informations sur Internet doit être contrôlé.

Le contrôle de l'information sur Internet est primordial, d'une part pour assurer la sécurité de l'Internaute, d'autre part afin de prévenir de toute dérive illégale.

Internet représente une source massive d'informations, mais également une source non négligeable de dangers : hameçonnages, chantages, usurpation d'identités… Utiliser Internet en soi n'est pas compliqué cependant la partie la plus difficile consiste à pouvoir identifier les menaces et à savoir comment les éviter. Le blocage de sites Internet ayant des comportements malveillants est essentiel, ou tout du moins mettre en garde les utilisateurs avant qu'ils n'y accèdent.

Pour ce qui est des dérives graves, Tor est un excellent exemple. Quasiment aucun contrôle n'est possible sur les sites hébergés accessibles depuis celui-ci. Le serveur est rendu anonyme, de la même façon que le client (cf. état de l'art). Rapidement après sa mise en service, il est passé d'un système révolutionnaire permettant de protéger son identité, outrepasser des blocages géographiques… à une nurserie des pires agissements de l'être humain : vente de drogue, d'armes, d'êtres humains, d'organes, de cartes bancaires volées, de faux papiers, location de botnets… Il est moralement discutable de voir ce genre de site fleurir publiquement sur Internet sans avoir de moyens pour les bloquer et prendre des mesures judiciaires contre leurs auteurs.

Le contrôle oui, mais il doit être encadré. La décision de censurer un site Internet ou de demander le retrait d'un contenu doit être prise sous le contrôle d'une autorité judiciaire, apte à prononcer un jugement. Actuellement en France, la décision de blocage d'un site Internet est prise par une « administration compétente ». Il n'est pas fait mention de justice et encore moins de jugement. Ceci peut entrainer des abus.

Il n'est pas possible de contrôler l'information sur Internet à 100%

Le contrôle total de l'accès aux informations sur Internet est une utopie.

Un site Internet ne peut être bloqué que partiellement. Les blocages complets de sites Internet complet se font en général soit sur le nom de domaine, soit sur l'adresse IP du serveur l'hébergeant.

Dans le premier cas de figure, il suffit à l'utilisateur de changer les serveurs qu'il utilise afin de faire la correspondance entre le nom de domaine et l'adresse IP du serveur. Les blocages administratifs de sites Internet sont effectués de cette façon en France. Les FAI doivent empêcher la résolution de certains noms de domaines via leurs serveurs DNS sur demande. Ce genre de blocage ne va impacter que les utilisateurs ne connaissant pas les manipulations à effectuer pour déjouer le blocage. Des instructions sont facilement trouvables via les moteurs de recherche.

Dans le deuxième cas, l'utilisateur, voulant à tout prix accéder à ce site, peut utiliser des moyens anonymisant, chiffrant son trafic (et donc sa requête) et sortant dans un autre pays qui, lui, ne va pas imposer de blocage. Cette dernière méthode s'adresse à une minorité d'utilisateurs informée.

Dans les deux cas, l'auteur d'un site bloqué peut également mettre en place différentes parades. The Pirate Bay est un site de téléchargement illégal, ayant vu le jour en 2003. Il est toujours accessible à l'heure où j'écris ces lignes. De nombreuses décisions de justice ont été prises contre lui, dans de nombreux pays, pour violation des droits d'auteurs entre autres. Des perquisitions ont été effectuées, peines de prison à l'encontre des fondateurs… Et aucun résultat probant. Les fondateurs ont été remplacés par d'autres personnes, par des mises en place de nombreux serveurs « miroir » à travers le monde… Impossible de bloquer tous les

noms de domaines secondaires et les centaines d'adresses IP utilisées. Cela bouge en permanence !

Même si des méthodes de déchiffrement du trafic des utilisateurs passant par des méthodes d'anonymisation viennent à apparaitre (ce n'est qu'une question de temps), d'autres technologies verront le jour peu de temps après que cette information soit connue. Il s'agit d'une course de fond ayant commencé il y a plusieurs millénaires, et qui n'est pas prête d'être finie.

La Corée du Nord nous montre un bon exemple d'incapacité à contrôler l'information à 100%. Le gouvernement met tout en œuvre pour éviter au maximum les contacts avec le reste du monde. Internet n'est accessible qu'à quelques élites du gouvernement. Et pourtant des informations filtrent… Il est possible de capter les signaux GSM des relais chinois proche de la frontière. Et même si ce n'était pas le cas, un téléphone satellite est capable de faire ceci depuis n'importe quel endroit du globe.

4.3 Préconisations

Mes préconisations concernant le respect de la liberté de l'information et le respect de la vie privée se découpent en quatre points.

Un Internet le plus libre et le plus neutre possible

Le seul moyen de préserver la liberté de l'information est de garantir la liberté d'accès au support qui la transmet, dans notre cas il s'agit d'Internet.

Le fait de surveiller massivement l'utilisation d'un moyen de transmission de l'information est une atteinte à la liberté et au droit à la vie privée. Si surveillance il y a, elle doit être fondée et ciblée.

Contrôle de l'information par décision de justice

Un Internet le plus libre et le plus neutre possible.

Oui, mais il doit tout de même être possible de contrôler la publication de certains contenus pouvant se révéler choquants, illicites, appelant à la haine et à la violence… Ces contenus doivent être bloqués du mieux possible ou supprimés, et leurs auteurs sanctionnés sur décision de justice. Ce doit être un juge qui doit prendre ces décisions, de façon juste et impartiale, sans être influencé de quelques façons que ce soit.

Surveillance ciblée

Le besoin de renseignement est primordial pour assurer le bon fonctionnement et la sécurité d'un état (intérieur et extérieur) ainsi que pour faire respecter les lois, mais doit être assouvi en tenant compte des libertés et des droits de chacun. Une surveillance de masse va à l'encontre

de cela.

Je préconise une surveillance ciblée et contrôlée par des décisions de justice afin d'éviter tout abus. Je pense que l'utilisation de « pots de miel » (de l'anglais honeypot) est un exemple approprié. La loi HADOPI utilise un dérivé de ce principe. Si une personne se fait prendre « la main dans le sac », c'est qu'elle aura probablement cherché à accéder au contenu de ce dernier. Une décision de justice doit bien sûr être prise afin de déterminer la culpabilité de la personne. Bien d'autres solutions existent.

Pendant longtemps ce fut appliqué avec les écoutes téléphoniques par exemple. Les abus qu'il y a eu éclatent régulièrement au grand jour et sont montrés du doigt. Pourquoi n'en est-il pas de même aujourd'hui, alors que l'information numérique est ancrée encore plus profondément dans notre vie privée ?

Sensibilisation et communication

Enfin, sensibiliser et communiquer pour faire prendre conscience au grand public des atteintes à ses droits et à ses libertés que nous subissons chaque jour, ainsi que leurs conséquences à court, moyen et long terme. Les exemples proposés dans ce document n'en sont qu'une infime partie.

Mais également sensibiliser et communiquer sur le monde du Libre (logiciels, services, données…). Il existe des solutions respectueuses de l'utilisateur.

Ceci doit être fait dès le plus jeune âge. Certes la suite Office de Microsoft est incontournable dans le monde du travail, mais qu'est-ce qui justifie un partenariat avec l'éducation nationale, si ce n'est de prendre en otage les jeunes cerveaux qui seront les acteurs du numérique de demain ?

Cette prise de conscience collective peut mener des gouvernements ou des géants du Net à revoir les méthodes qu'ils emploient. L'ère du numérique est encore jeune, à nous tous de la façonner.

4.4 Bilan

La liberté de l'information et le respect de la vie privée ne sont toujours pas des valeurs acquises, en France, mais également à travers le monde.

Il est compréhensible que nos données aient une valeur à la fois pour les géants du Net et pour les services de renseignements.
Il est compréhensible qu'elles puissent parfois apporter une valeur ajoutée non négligeable à l'utilisation d'un service par l'utilisateur auxquels elles appartiennent.
Il est compréhensible que les services de renseignements soient aveugles s'ils n'ont pas d'informations.

Mais ce genre de pratiques peut se révéler dangereux en cas d'abus, et quasiment rien ne peut nous garantir que ceci n'arrivera jamais.

Concernant la surveillance de masse, je suis persuadé qu'il existe des solutions moins couteuses et tout aussi efficaces, voire même plus. Bien sûr, à condition que le motif de cette surveillance soit bien celui que l'on nous communique. Ici nous pouvons appliquer le facteur d'ignorance.

Liberté, égalité, fraternité., voilà la devise de la République Française. De nombreuses personnes, par le passé, ont lutté et ont souffert pour faire reconnaitre ces trois mots comme une partie de notre identité commune. Ces trois mots sont une bonne définition à la notion de neutralité du Net. Ces trois mots ne sont jamais acquis définitivement.

Les progrès de la science et de la technologie nous rapprochent de plus en plus de l'avènement de l'ordinateur quantique. Beaucoup de savants sont d'accord pour affirmer que la première nation dans le monde à mettre la main dessus et à en maitriser son fonctionnement aura les moyens d'imposer une domination dans de nombreux domaines. Le chiffrement le plus robuste actuellement serait cassé en quelques minutes. De là en découle un contrôle total sur les

marchés économiques mondiaux, espionnage industriel massif, renseignement militaire… Jusqu'à ce que les défenseurs du chiffrement trouvent une nouvelle échappatoire.

4.5 Bilan personnel

La rédaction de cette thèse a énormément changé ma vision du monde numérique, même si la liberté de l'information et la neutralité du Net figurent dans la liste des sujets que je surveille avec attention depuis de nombreuses années.

Les deux dernières années furent particulièrement chargées en rebondissements dans le domaine : révélations de lanceurs d'alertes, climat d'insécurité en France suite aux attentats… Pas une semaine n'est passée sans une proposition de loi, la libération de documents sensible sur le sujet…

La partie la plus gênante à rédiger dans ce document fut probablement celle sur le facteur d'ignorance. Sans tomber dans la paranoïa et la théorie du complot, l'histoire nous montre clairement sa forte probabilité d'existence. Cela a remis en cause de nombreuses choses que je pensais acquisses, comme le fait de la sécurité apportée à mes propres données par les moyens de chiffrement moderne.

5. Annexes

5.1 Glossaire

« Deep package injection »

Méthode de surveillance des informations numériques. Il s'agit d'une analyse approfondie des paquets de données qui transitent sur un réseau. Cette méthode ressemble fortement à l'attaque « Man in the Middle ».

« Man in the Middle »

Attaque informatique visant à intercepter des informations. Il s'agit grossièrement de l'intrusion d'un utilisateur illégitime dans la chaine de transmission de requêtes informatiques. Il peut alors écouter le trafic et éventuellement le modifier à la volée.

Proxy

Il s'agit d'un composant logiciel permettant de faire l'intermédiaire entre un utilisateur et un service. Il permet de modifier l'adresse IP source visible par le destinataire.

TCP/IP

Protocole informatique permettant de transférer des données via des équipements réseaux.

TLS / SSL

Technologie de chiffrement de communications sur Internet (le fameux HTTPS en est un exemple d'utilisation). Elle permet également de vérifier l'identité de deux parties.

Tor / « Deep Web »

Technologie offrant la possibilité de chiffrer et de rendre anonyme des transactions d'informations. Certaines dérives sont malheureusement connues…

VPN

Réseau virtuel privé. Cette technologie sert à étendre un réseau physique, via un autre réseau

(Internet par exemple). Un VPN permet également de chiffrer et de rendre anonyme les échanges d'informations y transitant.

5.2 Bibliographie

Une brève note d'histoire

« Traité de documentation : le livre sur le livre, théorie et pratique », livre de Paul OTLET, éditions Mundaneum, 1934, page 428 à 431.

« L'Internet: Historique et évolution », site Internet planete.inria.fr, INRIA.

« Internet History Timeline: ARPANET to the World Wide Web », site Internet livescience.com, Live Science.

« Chronologie de l'histoire d'internet », site Internet sites.univ-rennes2.fr, Université Rennes 2.

« Internet History 1962 to 1992 », site Internet computerhistory.org, Computer History Museum.

« Brève histoire d'Internet », site Internet tuteurs.ens.fr, ENS/PLS.

« A Very Short History Of The Internet Of Things », site Internet forbes.com, Forbes.

Que se cache-t-il derrière ce terme « Internet » ?

« Networking Basics: What You Need To Know », site Internet cisco.com, Cisco.

« How Does the Internet Work? », site Internet web.stanford.edu, Stanford University.

« 1.7.les réseaux », site Internet rmdiscala.developpez.com, Developpez.

« Number Resources », site Internet iana.org, IANA

« HTTP (HyperText Transfer Protocol) - Basics », site Internet ntu.edu.sg, Nanyang Technological University.

Protection des données et anonymisation

« Histoire des codes secrets », livre de Simon SINGH, éditions Le livre de poche, 2001.

« La stéganographie », PDF publié sur le site Internet univ-orleans.fr, Université d'Orléans.

« Chiffrement et Stéganographie », site Internet korben.info, Korben.

« Steganography: Hiding Data Within Data », site Internet garykessler.net, Gary C. Kessler.

« Classical Cryptography », site Internet cs.uri.edu, University of Rhode Island.

« Transposition Ciphers », site Internet cs.utexas.edu, University of Texas at Austin, Department of Computer Science.

« The Caesar Cipher », site Internet cs.trincoll.edu, Trinity College.

« The Caesar Cipher and Modular Arithmetic », site Internet math.stonybrook.edu, Stony Brook University, Mathematics Department.

« Cracking Classic Ciphers », site Internet rivier.edu, Rivier University.

« Classical Ciphers and Frequency Analysis Examples », site Internet sandilands.info/sgordon/, Steven GORDON.

« Vigenere Cipher », site Internet nctm.org, National Council of Teachers of Mathematics.

« The Vigenère Cipher Encryption and Decryption », site Internet cs.mtu.edu, Michigan Technological University, Computer Science Department.

« The Vigenère Cipher: Frequency Analysis », site Internet cs.mtu.edu, Michigan Technological University, Computer Science Department.

« Enigma Cipher Machines », site Internet cryptomuseum.com, Crypto Museum.

« The Enigma cipher machine », site Internet codesandciphers.org.uk, Codes and Ciphers.

« Asymmetric-Key Cryptography », site Internet cs.cornell.edu, Cornell University, Department of Computer Science.

« Past, present, and futur methods of cryptography and data encryption », PDF publié sur le site Internet eng.utah.edu, The College of Engineering at the University of Utah.
« The Enigma cipher machine », site Internet codesandciphers.org.uk, Codes and Ciphers.

« The NSA and Weak-DH », site Internet lawfareblog.com, Lawfare.

Mondialisation des informations et législations locales

« Economie numérique et mondialisation : des vecteurs de croissance et de liberté ? », site Internet arcep.fr, ARCEP.
« Mondialisation et Internet », site Internet henricapitant.org, Association Henri Capitant.

Profilages, censures, filtrages et désindexations

« surveillance://: Les libertés au défi du numérique : comprendre et agir », livre de Tristan Nitot, aux éditions C&F Éditions, 2016.

« Le profilage des individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données », PDF publié sur le site Internet coe.int, Conseil de l'Europe.
« Le profilage et la publicité ciblée », PDF publié sur le site Internet cai.gouv.qc.ca, Commission d'accès à l'information du Québec.
« Online Profiling », site Internet computerworld.com, Computer World.
« Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law », PDF publié sur le site Internet ivir.nl, Institute for Information Law.

« Les 10 pays qui exercent la censure la plus forte », site Internet cpj.org, Committee to Protect Journalists.

« Censure du Net », site Internet laquadrature.net, la Quadrature du Net.

« Chine : la Grande Muraille électronique à son apogée », site Internet 12mars.rsf.org, Reporters sans frontières.

« Les Pays-Bas inscrivent la neutralité du Net dans la loi », site Internet lemonde.fr, le Monde.

« Google, le blacklistage et la censure », site Internet infonum.iut.u-bordeaux-montaigne.fr, IUT Bordeaux Montaigne.

Droit à la vie privée

« Déclaration universelle des droits de l'homme », site Internet un.org, Nations Unies.

« Convention européenne des droits de l'homme », site Internet echr.coe.int, Cour européenne des droits de l'homme.

« Charte des droits fondamentaux de l'Union européenne », site Internet europarl.europa.eu, Parlement européen.

« Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29 », site Internet cnil.fr, Commission nationale de l'informatique et des libertés.

Actualités internationales

« Revelations », site Internet edwardsnowden.com, Edward SNOWDEN.

« Edward Snowden: how the spy story of the age leaked out », site Internet theguardian.com, The Guardian.

« Edward Snowden Fast Facts », site Internet edition.cnn.com, CNN.

« Profile: Edward Snowden », site Internet bbc.com, BBC.

« Inner workings of a top-secret spy program », site Internet apps.washingtonpost.com, The Washington Post.

« NSA Prism program taps in to user data of Apple, Google and others », site Internet theguardian.com, The Guardian.

« XKeyscore : NSA's Google for the World's Private Communications », site Internet theintercept.com, The Intercept.

« Synthèse du programme de surveillance américain », site Internet linuxfr.org, LinuxFr.

Actualités nationales

« LOI n° 2015-912 du 24 juillet 2015 relative au renseignement », site Internet legifrance.gouv.fr, Legifrance.

« Projet de loi relatif au renseignement », site Internet assemblee-nationale.fr, Assemblée Nationale.

« Loi relative au renseignement », site Internet senat.fr, Sénat.

« Loi Renseignement », site Internet wiki.laquadrature.net, la Quadrature du Net.

« Le point de vue d'OVH.com sur la loi renseignement », site Internet ovh.com, OVH.

« Projet de loi Renseignement », site Internet sous-surveillance.fr, Sous-Surveillance/la Quadrature du Net.

« Facebook follows Google with tough encryption standrad », site Internet theverge.com, The Verge.

« Bernard Cazeneuve veut « une initiative européenne » contre le chiffrement », site Internet lemonde.fr, Le Monde.

« Contre le chiffrement, le dangereux projet de Cazeneuve », site Internet lepoint.fr, Le Point.

« La Cnil et le Conseil national du numérique défendent le chiffrement des communications », site Internet lefigaro.fr, Le Figaro.

« Tristan Nitot : "Restreindre le chiffrement affaiblirait la démocratie" », site Internet franceinter.fr, France Inter.

« Contrôler le chiffrement : un calcul difficile pour le gouvernement », site Internet liberation.fr, Libération.

« surveillance://: Les libertés au défi du numérique : comprendre et agir », livre de Tristan Nitot, aux éditions C&F Éditions, 2016.

« Histoire des codes secrets », livre de Simon SINGH, éditions Le livre de poche, 2001.

Le facteur de l'ignorance

« Histoire des codes secrets », livre de Simon SINGH, éditions Le livre de poche, 2001.

« Cryptologie : art ou science du secret ? », site Internet ssi.gouv.fr, ANSSI.

5.3 Résumés des interviews

5.3.1 Interview de Christophe BRAND

Penses-tu que le renseignement de masse est pertinent et efficace ?
Par exemple en France, la « loi renseignement » fait état de dispositifs appelés « boites noires » qui permettent de recueillir les métadonnées de toutes les connexions effectuées depuis le territoire Français et de les conserver pendant une durée de 30 jours.

Je pense qu'avec les outils que nous avons aujourd'hui on peut faire du renseignement de masse. Ça ne veut pas dire que c'est la seule source de renseignement. Typiquement, les impôts font un traitement de masse de l'information qu'ils ne faisaient pas avant et ça devient très efficace. Quand ils décident de faire un contrôle, ils ont 90% de chances d'aller au bon endroit. La question c'est effectivement d'avoir une combinaison efficace entre du renseignement de masse, des renseignements de terrain et d'avoir des moyens pour croiser et analyser tout ça. Néanmoins, je ne pense pas qu'une personne malintentionnée expérimentée va tomber dans le piège d'envoyer des informations sensibles en clair via les réseaux de communications standard. Donc efficace oui, si les bons filtres sont appliqués et complétés par d'autres sources d'informations. Après, que 99,999% des données récoltées soit sans valeur car les personnes ayant quelque chose à se reprocher utilisent certains moyens pour passer à travers les mailles du filet… Reste 0,001% qui peuvent être des renseignements bien utiles pour la sécurité nationale.

Le fait que cette collecte d'informations est non ciblée et puisse porter atteinte à la vie privée ne te dérange pas ?

La question est comment ça va être géré. Si c'est une machine qui analyse ses informations, bien sécurisée… Me concernant, je ne suis pas inquiet des informations qui pourraient remonter

et du moment qu'aucune analyse moralement discutable sur mes opinions politiques… Et encore, même ça, je n'ai rien à me reprocher.

Quand je parlais de vie privée, je faisais allusion à des informations qui sont habituellement partagées avec un nombre restreint de personnes : des amis proches, de la famille, un(e) conjoint(e)… Le fait de vouloir maitriser la diffusion d'une information ne fait pas d'elle qu'elle est illégale et répréhensible.

L'information en question n'est pas publique. Elle est collectée par le gouvernement à des fins d'analyse et de renseignement. Et même si quelques personnes sont amenées à en prendre connaissance, tant que c'est dans un cadre défini comme la loi renseignement et que la finalité est connue, je n'ai pas de problème avec ça. On peut comparer ça au contrôle radar : je roule aux limitations de vitesse, ils me contrôlent, je n'ai rien à me reprocher. Donc personnellement, ça ne me pose aucun problème, après sur le plan moral (Big Brother…), oui c'est dérangeant, mais si ça peut éviter des événements comme le Bataclan…

Donc, tu n'as rien à cacher ?

Non, rien à cacher au gouvernement.

Google récupère des infos sur notre navigation, Amazon dresse un profil de chaque acheteur, Facebook collecte des informations données de notre plein gré, certaines assurances distribuent des trackers d'activité… Cette récolte massive de nos informations du quotidien par les géants commerciaux du Web te dérange-t-elle ?

Oui. De nombreuses pratiques vont trop loin. Que le gouvernement le fasse à des fins de sécurité, soit, je n'y suis pas opposé. En revanche, personne n'est en mesure de contrôler ces entreprises, les informations qu'elles récupèrent et ce qu'elles en font. Je suis persuadé que nous ne savons pas tout. Qui nous dit que Facebook, entreprise américaine prospère, n'est pas

« encouragée » par la NSA. Quelle aubaine que ces millions d'utilisateurs à travers le Monde publient de leur plein gré des informations aussi précises sur leurs vies privées, où autrefois les services de renseignements devaient enquêter pendant de très longues périodes sur le terrain pour les obtenir ! Les smartphones également. Petit objet technologique dont les utilisateurs sont de plus en plus dépendants. Traces GPS, caméras, micros… Un véritable réseau d'informations accessible en temps réel partout sur le globe. Outre ces aspects-là, si ce profilage peut fournir des publicités pertinentes…

Penses-tu que le modèle de législation actuel est pertinent ? Je m'explique. Internet c'est la mondialisation de l'information, mais chaque pays possède sa propre législation. Toutes ces différentes législations rentrent souvent en contradiction les unes avec les autres, sur de nombreux sujets. Il suffit à une personne voulant commettre un acte comme étant reconnu comme étant un délit dans son pays d'habitation de passer par un VPN, afin d'avoir un point de sortie dans un pays tolérant cet acte pour éviter toute sanction. Il serait peut-être pertinent de pouvoir harmoniser tout ça.

Oui, effectivement, il y a un manque de logique dans la chose. Mais avoir un organisme, une entité… Neutre, impartiale et surtout efficace, c'est de l'utopie. Il suffit de regarder les accords mondiaux sur l'environnement, l'ONU… C'est très compliqué de les faire appliquer par tous et les sanctions sont dérisoires.

5.3.2 Interview de Bertrand DESPREZ

Penses-tu que la surveillance de masse (en général) est efficace et pertinente ?

La surveillance de masse n'est pas pertinente. Même si on met des caméras de vidéos surveillance partout, il y aura toujours des événements qui arriveront. Recueillir l'information c'est une chose, l'analyser de façon pertinente en est une autre. Elle est intrusive, c'est tout.

La surveillance de masse n'est pas efficace. Il y a toujours des moyens de passer sous les radars. Prenons Hadopi par exemple. On a voulu surveiller les téléchargements illégaux. Au moment où ils ont voulu le mettre en place, les solutions pour y échapper existaient déjà. Le plus dramatique dans l'histoire, c'est qu'ils ont presque publié dans les médias comment ils allaient s'y prendre pour identifier les personnes qui téléchargeaient. On parle de sécurité ! La première chose à faire c'est de ne rien divulguer sur les méthodes qui seront employées. Inefficace. Quitte à faire de la sécurité, autant le faire bien, n'en parler à personne.

En revanche, oui il faut de la surveillance, mais de la surveillance ciblée sur certains individus.

Penses-tu qu'il est possible d'avoir un Internet libre, sans aucune surveillance et sans aucun contrôle (censure…) des informations qui y transitent ?

Le but premier d'Internet à sa création était de pouvoir échanger des informations. Des informations touchant aux domaines militaire et scientifique dans un premier temps. L'utilisation d'internet a ensuite été élargie au grand public. A cette époque il n'était pas question de surveillance ou de contrôle. Maintenant, les entités qui se privent de le faire ont un gros désavantage. Leurs concurrents n'hésiteront pas à le faire si cela peut leur permettre de prendre l'avantage. Donc, tout le monde surveille et glane les informations qu'ils peuvent.
Pour ce qui est du contrôle… Oui, probablement qu'il faut contrôler les informations qui y sont accessibles. Le principe de base était bien, mais Internet n'était pas destiné à être accessible à autant de monde. On y trouve aujourd'hui de tout. Certaines choses peuvent être dangereuses.

Penses-tu que le droit à la vie privée est révolu ?

Oui. Toutes personne qui a un smartphone y a renoncé. Avec l'avènement de l'ultra-communication et de l'ultra mobilité, nombre de nos informations personnelles ne nous appartient plus entièrement. Sans même parler de Google, Facebook… Tu tapes ton nom dans un moteur de recherche, tu vas trouver plein de photos de toi que tu n'as jamais mis sur le Net.

D'autres personnes que tu connais (ou pas) s'en seront chargés avec leurs téléphones portables.

Est-il normal, pour toi, que l'utilisation d'Internet soit régie par autant de législations qu'il y a de nations dans le monde, alors que l'essence même d'Internet est la mondialisation de l'information ?

L'Européaniser… L'Europe a essayé, ça ne marche pas. Le mondialiser… Encore moins. Vas t'amuser à négocier avec la Chine, la Corée du Nord, l'Arabie Saoudite... Chacun à des intérêts différents, personne n'arrivera à se mettre d'accord.

C'est à toi de maitriser les informations qui sont diffusées sur toi. Ne pas utiliser de smartphone, ne pas utiliser Facebook, Google… Les gouvernements et les gros groupes qui ont des bénéfices financiers grâce à leurs services ne te demanderont pas ton avis. Faire ces sacrifices, ou vivre avec, ce sont les deux seules solutions.

5.3.3 Interview de Pierre-Yves PARIS

Pensez-vous qu'il est primordial de veiller au contrôle de l'information sur Internet ?

La surveiller oui, la contrôler c'est autre chose. Sous la forme de contrôles il y a bien souvent une forme de censure qui va avec. Si une information doit être censurée, il faut que ce soit fait à travers les tribunaux. Par exemple Google, Facebook, Twitter et les autres grosses entreprises du Net censurent rarement d'eux-mêmes les contenus qui circulent sur leurs plateformes, contrairement à ce que l'on pourrait croire. Souvent, quand cela arrive, c'est qu'une autorité juridique en a fait la demande.

À mon avis il faut continuer à pouvoir s'exprimer librement sur tous les sujets, mais d'un autre côté il ne faut pas que ça rentre en contradiction avec les lois d'un pays, quel qu'il soit.

Un exemple d'actualité, les sites prônant des idéaux religieux. Une personne revendiquant avec ferveur son appartenance à la religion de l'Islam en a tout à fait le droit, tant que ses propos ne vont pas enfreindre des lois ou inciter des gens à commettre des actions illégales. C'est l'incidence de ces propos qu'il faut estimer plus que les propos eux-mêmes.

Pensez-vous que la surveillance de masse est pertinente et efficace ?

On n'a pas de notion d'efficacité et je pense que l'on n'en aura jamais. Si l'on nous donne un exemple, c'est nous dire comment ils ont fait pour tel ou tel évènement déjoué et il ne faut surtout pas savoir comment les forces de l'ordre opèrent, d'autres personnes malintentionnées pourraient se servir de ces éléments pour éviter de tomber dans le même piège.

Oui, je pense que ça peut être efficace. Là aussi il faut que ce soit très bien cadré et dans un but particulier qui, en France, à l'heure actuelle est de lutter contre le terrorisme. L'accès aux informations ainsi collectées doit se faire sous contrôle de la justice. La surveillance de masse existe depuis longtemps, les lois récentes n'ont fait que l'officialiser.

Au vu de cette surveillance de masse (pas uniquement en France, mais à l'échelle mondiale), l'exploitation de nos données par les géants du Net… Pensez-vous que le droit à la vie privée est révolu ?

Il a changé. Mark ZUCKERBERG disait il y a quelques années, il faut que la population mondiale change son regard sur la vie privée, car elle a évolué. C'est de plus en plus compliqué de la préserver avec les moyens électroniques. La vie privée devient virtuelle. Pratiquement tout ce qui peut être transformé en 0 et en 1 devient public. Je pense qu'elle n'existe plus vraiment.

Pour la surveillance par notre gouvernement, des lois nous protègent… Mais ce qui reste encore le plus efficace est la masse de ces informations. Une information privée va être noyée dans cette masse et il va être difficile de la trouver. Je pense que notre vie privée est protégée de ce

côté-là dans la mesure où les forces de l'ordre ont probablement autre chose à faire de leurs journées.

D'un autre côté, il y a les gros groupes qui peuvent être intéressés. Google, Facebook… Quand il y a de l'argent en jeux, il n'y a plus grand-chose d'autre qui compte pour eux. C'est probablement ce qui est le plus dangereux à mon avis. Ils ne sont pas soumis aux lois françaises. Ils se permettent de conserver nos données sans limites de temps et on ne sait pas précisément comment ils les exploitent pour faire des profits.

Pensez-vous que la mondialisation de l'information offerte par Internet est compatible avec des législations différentes pour chaque pays ?

Chaque pays à ses particularités : politiques, culturelles… Et donc doit avoir un droit à s'opposer à certaines choses. La mondialisation n'a pas que du bon. Même si une entité devait prendre le contrôle de ça, même si elle est apolitique, si elle prône la neutralité du Net (ce qui pourrait être une très bonne chose), il ne faudrait pas qu'elle supprime la possibilité d'adapter les règles en fonction de chaque pays. Sauf cas particulier, la plupart des gouvernements dans le monde sont là pour aller dans le sens de leurs peuples, ainsi que de le protéger. Si on prend l'exemple de la CNIL, elle nous défend régulièrement contre des entités étrangères. Sans elle nous serions quasiment sans défense. Sans ces particularités locales, très rapidement, ce serait les sociétés commerciales qui prendraient le dessus.

Pensez-vous qu'il est facilement possible pour qui le veut de contourner ces problématiques de législation et de surveillance ?

Bien sûr. Toujours ! On peut considérer qu'il y a de nombreuses solutions, accessibles facilement et qui apportent une certaine garantie de sécurité pour contourner toutes ces mesures. Bien sûr, il n'est pas exclu que ce ne soit plus le cas et que nous soyons dans l'ignorance. C'est le jeu du chat et de la souris, qui dure depuis la nuit des temps.

Pensez-vous que le logiciel libre a une chance face aux gros bonnets du Net ?

Non. J'ai eu de gros espoirs il y a 20 ans face à Microsoft. Résultat aujourd'hui, malgré des systèmes d'exploitation et des logiciels de qualité, ça n'a pas pris. En face, les gros lobbys passent des accords avec des fabricants de machines. Acheter un ordinateur sans OS, même à l'heure d'aujourd'hui ça reste compliqué, peu de fabricants ont franchi ce cap. Le particulier qui achète un ordinateur veut pouvoir l'utiliser en le sortant de la boite, sans savoir ce qui se passe sous le capot. L'administration française a essayé de passer sur des systèmes d'exploitation et des logiciels de bureautique libre, mais les moyens de formations du personnel n'ont pas été mis derrière. Résultat, c'est un échec. Les gens de Framasoft mènent depuis de nombreuses années des campagnes dans ce sens : apporter des alternatives aux services et logiciel propriétaire par des solutions libres. Si on prend les 140 000 utilisateurs d'Airbus Group : combien connaissent le nom de cette association ? Une minorité. Ceci étant, le libre existera toujours. Il y aura toujours des gens avec cette conscience du logiciel libre. Dans ce sens Framasoft est un succès, malgré qu'il soit limité. Ça ne prendra jamais une ampleur énorme. Une entreprise qui opte pour du libre est courageuse. Une entreprise qui achète un produit commercial a un support en cas de dysfonctionnement, ce qui est rarement le cas si c'est gratuit.

La Quadrature du Net

thanks for his/her support

Pierre-Benoît JOUBERT

and awards him/her the digits 176131001 *to* 176132000 *of* π

3.14159265358979323846264338327950288419716939937510582097494459 2...

...29196230722641304783763210344606197493452995447806388977284497454436255573214131488590109220197370089854722751401416194729781706154581973394594208680047264914400259662772943484949588317792540824548611607004561780313273665097289561566175618652570280466478164262814994560143901598386063416244077913158071095067325452878287290602697021491225675828916003391417761967257540007260868645682431209746727271717116522393422060498261214894798437711895943307754134567128087739312476696024182800097447265190682088331939833545489387416500290246101035210039561176518291387397284152334347432628738975483839377329232932974179241048936733874898602107409009308843756346170994378386619888399977554765401347346475636686732656357044976239773302790319512096160862555747700091997440662273543740169588493607206979274548119838120029026936638930339100355996367522084316497796126446879792683542203165615592126648093626108585289740209053372065525962045476696816700890631661942853661914818873573322343105381521399527161 3...