Connectez-moi !

Martin Untersinger

Préface de Benjamin Bayart

# ANONYMAT sur INTERNET

## Protéger sa vie privée

2e édition

EYROLLES

# ANONYMAT sur INTERNET

2e édition

## Protéger sa vie privée

**L'équilibre entre vie privée et vie publique tend à s'inverser : publier ne coûte rien, préserver sa vie privée requiert des efforts.**

**Dans le même temps, la notion d'anonymat sur Internet est souvent mal comprise. Quel est son intérêt ? Pourquoi faut-il en préserver la possibilité, malgré les dérives ?**

La deuxième édition de cet ouvrage consacre un chapitre dédié à l'anonymat des mobinautes qui surfent sur Internet via des smartphones et tablettes. Elle propose également un regard nouveau sur les révélations faites par l'ex-agent de la NSA Edward Snowden.

Martin Untersinger est journaliste spécialisé dans les questions liées à Internet et notamment celles de la vie privée et de la surveillance. Parallèlement à ses études à Sciences Po Paris, il a travaillé pour le site d'information spécialisé dans les questions numériques OWNI, pour Lemonde.fr et pour Rue89. Son article sur l'anonymat a fait l'objet de plus de 180 000 lectures.

Anonymat relatif et partiel. Vie publique versus vie privée. Traces invisibles. Pseudonymat. Pression de l'État. Données de connexion. Trackers. Surveillance par les entreprises. Tablettes. Liberté d'expression. Se Protéger. Estimer le risque. Navigateur. Smartphones. Exil des données privées sur le Cloud (Google, Facebook...). Disparaître du Web. Pistage des réseaux sociaux et publicitaires. Vulnérabilités Chiffrement. PGP et OTR Proxy VPN Tor. Anonymous. Cyberdissidence. Protéger SMS et appels. Droit à l'oubli.

Connectez-moi !

*Démystifier les rouages de la société numérique.*

www.editions-eyrolles.com

Code éditeur : G14021
ISBN : 978-2-212-14021-7

# ANONYMAT *sur* INTERNET

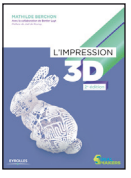
## Protéger sa vie privée

## Chez le même éditeur












Retrouvez aussi nos livres numériques sur
**http://izibook.eyrolles.com**

Connectez-moi !

Martin Untersinger

Préface de Benjamin Bayart

# ANONYMAT sur INTERNET

## Protéger sa vie privée

2e édition

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

# Préface

C'est devenu une banalité, fausse, que de dire qu'Internet est en train de changer nos sociétés. Sauf à lui supposer une origine divine, Internet n'a pas été imposé à la société depuis l'extérieur ni n'est en train de la réformer contre son gré. Internet est l'outil dont les sociétés humaines occidentales se sont dotées pour évoluer, pour changer. Ce changement prend bien des formes, et touche bien des aspects, dont les mieux compris et analysés touchent à l'échange de biens immatériels et à la liberté d'expression.

Concernant l'échange des biens immatériels, par exemple le partage de fichiers musicaux ou de vidéo, la caricature du vol souvent employée n'a pas de sens, puisque l'ancien exemplaire du fichier est *toujours* sur le disque dur où il se trouvait auparavant. Si le fait de regarder la baguette de pain dans la vitrine en fait apparaître, magiquement, une nouvelle dans ma main, je ne vole pas le boulanger. Cet échange de biens immatériels a des conséquences sur les modèles économiques de nombreuses industries, à commencer par celle du divertissement. Quand on fait métier de vendre des copies sur support plastique, comment survivre à l'apparition de la fantastique machine à copier qu'est Internet ?

Quant à la liberté d'expression, c'est simplement le fait que chaque citoyen puisse s'exprimer publiquement, et ait l'opportunité d'être lu et entendu par tous. Au siècle dernier, protéger la liberté d'expression, c'était protéger la liberté de la presse. La seule forme d'expression accessible au commun était alors la discussion autour de la table au dîner de Noël, ou au café du coin. Ce qui était, au siècle dernier, réservé à une minorité (journa-

listes, artistes, dirigeants divers, etc.) est maintenant accessible à tous. Quiconque a un mur Facebook, un blog, un compte Twitter, un tumblr, dispose d'un lieu d'expression qu'il peut ouvrir au public. Sur Internet, tout le monde est éditeur de ce qu'il publie, tout le monde est éditorialiste et chroniqueur. La question des libertés, et des règles de société, qui vont avec cette expression publique, est une question majeure de l'organisation des sociétés post-Internet, une question politique : comment voulons-nous faire société ensemble ?

Cette question se décline en de nombreuses facettes. À commencer par celle du pouvoir qu'ont certains intermédiaires techniques sur notre vie numérique. Tout ce que je dis et fais sur Internet passe par mon fournisseur d'accès. Quel pouvoir de censure a-t-il ? Quel pouvoir d'intrusion a-t-il ?

C'est une des premières questions que je me suis posées sur le sujet, il y a plus de 15 ans. J'y ai répondu en ayant un accès Internet dans une association loi 1901, FDN, ce qui à l'époque était classique. J'y ai répondu en reprenant la présidence de l'association pour qu'elle ne disparaisse pas, pour que l'accès à Internet ne soit pas forcément une marchandise, et qu'il continue de pouvoir être autre chose qu'une marchandise. Et en étant toujours, en 2013, dix-sept ans plus tard, abonné d'un fournisseur d'accès associatif.

Les intermédiaires techniques sont nombreux à avoir un fort pouvoir de nuisance dans le monde numérique. Outre le fournisseur d'accès, il y a également le fournisseur de l'ordinateur (que ce dernier ait la forme d'un téléphone n'y change rien), ou le fournisseur de logiciel. Ces questions-là sont anciennes également. Pour ma part, j'ai fait le choix évident du logiciel libre précisément pour ces raisons : *mon* ordinateur fait ce que *je* veux, plutôt que ce qu'un éditeur a choisi qu'il fasse pour des raisons qui ne sont pas les miennes.

Les grandes plates-formes de services sont finalement d'apparition plus récente, au milieu des années 2000. Mais leur place

au cœur de l'expression publique de chacun devient centrale et donc dangereuse. Là aussi, la question qui revient est toujours la même : qui est capable de décider, qui peut censurer, qui rend des comptes ? Au final, est-ce moi qui suis libre de m'exprimer, ou est-ce Twitter qui tolère ce que je dis aussi longtemps que ça l'arrange ?

Enfin, il y a la question de l'identité, encore mal comprise. Pourtant, les personnes qui s'expriment publiquement ont toujours pu le faire sous une identité qu'ils ont choisie, sculptée, choisissant le nom, mais aussi la personnalité qu'ils montrent au public. Pour preuve l'exemple simple de Johnny Hallyday, dont tout le monde se fiche de savoir qu'il s'appelle J.-P. Smet. Et ce n'est pas un privilège d'artiste. On peut également se faire élire président de la République sous un pseudonyme, comme ce fut le cas de Nicolas Sarközy de Nagy-Bocsa, élu sous le nom de Nicolas Sarkozy, sans tréma ni particule. Même le président des États-Unis est connu dans le monde entier sous le nom de Bill Clinton, alors que son prénom est William. Jusqu'au Pape, qui règne sous un faux nom.

Lorsqu'on prend la parole en public, on choisit le nom sous lequel on apparaît. Cette identité-là n'est pas forcément celle de l'état-civil, mais c'en est bien une. Qui, d'ailleurs, ne connaît quelqu'un dont le prénom dans la vie courante diffère de ceux inscrits sur sa carte d'identité, ou n'est pas le premier de ceux-là, ou encore n'est pas orthographié de même ?

Les identités sous lesquelles on souhaite apparaître peuvent être multiples, et pour de multiples raisons. On peut par exemple ne pas avoir le même nom dans un réseau militant (Chaban) et dans le monde politique (Delmas). Le choix de l'identité sous laquelle chacun s'exprime, en fonction du lieu et du contexte, relève des libertés attenantes à la liberté d'expression. Et ce droit relève, forcément, du droit de s'exprimer sans donner de nom, du droit à l'anonymat.

La question des identités, à l'heure du numérique et donc de la surveillance généralisée, est une question politique clef, une question majeure sur la façon dont nous voulons faire société. J'en prend un exemple simple : l'Assemblée Générale qui m'a élu président du Fonds de Défense de la Neutralité du Net l'a fait sans voir mes papiers d'identité. C'est l'individu qui s'exprime dans l'espace public sous le nom de Benjamin Bayart, reconnaissable à sa barbe et à ses cravates ridicules, qui a été élu à ce poste. Pourtant, c'est à la carte d'identité que le banquier a accordé la signature sur un compte bancaire. D'une certaine façon, le banquier n'a pas respecté le vote de l'Assemblée Générale, pourtant souveraine sur la question. Il a supposé que le Benjamin Bayart de l'état-civil était le même que celui de l'espace public.

Une forme numérique assez simple est pourtant au point depuis vingt ans : ma clef de chiffrement publique, qui est... publique. L'Assemblée Générale aurait pu élire comme président « la personne qui s'exprime avec cette signature », et le banquier aurait pu contrôler cette information, bien plus fiable que ce que raconte le support de plastique distribué par l'État. Ainsi il m'appartient de savoir et de faire savoir qui je suis, il m'appartient de me nommer, et l'état-civil ne sert qu'à enregistrer celui de mes noms qui servira dans mes échanges avec l'administration, ou lors du prochain recensement.

Les questions autour des identités, autour de l'anonymat qui en est le corollaire immédiat, autour du droit de ne pas être surveillé, autour du droit à la vie privée, sont des questions majeures pour comprendre la société qui est en train de se construire avec Internet. Et c'est une des questions qui restent le plus mal connues, même des spécialistes.

Benjamin Bayart

Président de l'association French Data Network

# Table des matières

**Avant-propos . . . . . XVII**
Pourquoi ce livre ? . . . . . XVII
Plan de l'ouvrage . . . . . XXI
Remerciements . . . . . XXII

**1. Anonymat sur Internet : de quoi parle-t-on ? . . . . . 1**
Bien définir l'anonymat . . . . . 1
Un anonymat tout relatif . . . . . 2
Sur Internet, l'anonymat ne cache qu'une partie de son identité . 3
Neutralité (morale) de l'anonymat . . . . . 3
Définition de la vie privée . . . . . 3
La vie privée, une nécessité selon Montaigne . . . . . 3
La vie privée numérique, c'est le contrôle . . . . . 5
Problème : on n'a pas toujours le contrôle . . . . . 5
Pourquoi Internet chamboule tout ? . . . . . 7
Internet berceau de la vie publique . . . . . 7
Un renversement : une vie publique par défaut, privée seulement parfois . . . . . 7
Traces involontaires et invisibles . . . . . 8
Le pseudonymat . . . . . 9

**2. Sur Internet, l'anonymat n'existe pas . . . 11**
Une pression croissante de l'État . . . . . 11
Pour contrôler, il faut savoir qui est qui et qui fait quoi . . . . . 13
Un exemple français : la conservation des données de connexion . . . . . 14
Comment ça marche ? . . . . . 16

L'anonymat remis en question pour des intérêts économiques . . . 17
Valeur des données personnelles pour les « e-commerçants » . . 18
Un modèle économique reposant sur votre identité… . . . . . 19
… donc hostile à l'anonymat et au pseudonymat . . . . . 20
L'anonymat, un obstacle au modèle économique du Web . . . . . 21
Un dilemme insurmontable : communiquer ou laisser des traces ? . . . . . 23
La menace des « trackers » publicitaires . . . . . 23
Comment les entreprises font-elles pour vous surveiller ? . . . . . 24
Où se cachent les mouchards ? . . . . . 25
Les données collectées par les trackers sont anonymisées : un mythe ? . . . . . 26
Les données ne sont jamais anonymes . . . . . 27
Des critiques de films peuvent révéler une identité . . . . . 27
Identification par des requêtes dans un moteur de recherche . . 28
Le dossier médical d'un gouverneur identifié . . . . . 29
Les informations publiées sur le Web nous font-elles courir à notre ruine ? . . . . . 30

**3. De l'intérêt de l'anonymat . . . . . 33**

L'anonymat, une histoire de contrôle . . . . . 34
Être qui on veut . . . . . 34
Le pseudonymat . . . . . 35
L'anonymat et la liberté . . . . . 36
L'anonymat, nécessaire à la liberté d'expression ? . . . . . 36
L'anonymat protégé par la justice . . . . . 37
L'argument « Je n'ai rien à cacher » . . . . . 39
Un argument un peu absurde . . . . . 39
Trois exemples pour le réfuter . . . . . 40
Les choses commencent à changer . . . . . 42
L'anonymat et le droit . . . . . 43
Qu'est-ce que la vie privée ? . . . . . 44
Des dispositions plus précises dans d'autres textes juridiques . . 45
Vers un véritable droit à l'anonymat ? . . . . . 46

Le droit est parfois mal adapté . . . . . 46
Typologie des menaces . . . . . 47
Les entreprises . . . . . 47
L'État et la police . . . . . 49
Piratage et défaillances . . . . . 50
Vos proches . . . . . 51

**4. Les bases de la protection . . . . . 53**

Identifier ses ennemis et estimer le risque . . . . . 53
Les six menaces pour votre vie privée . . . . . 54
Différencier risque et menace . . . . . 55
Les cinq commandements de l'anonymat . . . . . 56
Être anonyme : se protéger d'une menace inconnue . . . . . 58
L'anonymat dépend des autres . . . . . 58
Un échange, plusieurs vulnérabilités . . . . . 59
Les questions à se poser . . . . . 60
Le navigateur . . . . . 62
Naviguer, qu'est-ce que c'est ? . . . . . 62
Quel navigateur choisir ? . . . . . 64
Pourquoi importe-t-il de protéger son navigateur ? . . . . . 65
Ne pas laisser de traces avec son navigateur . . . . . 67
Désactiver ou supprimer l'historique de navigation . . . . . 68
Mode navigation privée . . . . . 69
Cookies . . . . . 70
« HTTPS everywhere » . . . . . 72
Les requêtes HTTP . . . . . 75
L'adresse IP . . . . . 76
D'autres outils plus complexes pour dissimuler les traces du navigateur . . . . . 77

**5. Géants et entreprises du Web . . . . . 79**

Comment savoir quelles traces j'ai laissées ? . . . . . 80
Traces volontaires . . . . . 81
Traces involontaires . . . . . 81

Évaluer les risques en souscrivant à un service . . . . . 82
Conditions générales d'utilisation, « terms of service » et politiques de vie privée . . . . . 82
Les questions à se poser avant d'utiliser un service . . . . . 85
Protéger son identité chez les géants du Web . . . . . 86
Le cas Google . . . . . 87
Disparaître du Web (et récupérer ses données) . . . . . 90
Faire une dernière sauvegarde . . . . . 91
Peut-on faire confiance à un géant du Web ? . . . . . 92
Déjouer le pistage à notre insu. . . . . 94
Empêcher les réseaux sociaux de nous suivre . . . . . 94
Empêcher les publicitaires de nous suivre . . . . . 96
Quelques principes avant de télécharger une extension ou un programme . . . . . 100

**6. Communiquer : e-mails et discussions instantanées . . . . . 103**

Qu'est-ce qu'un e-mail ? Comment circule-t-il ? . . . . . 103
Un peu de vocabulaire . . . . . 104
Différence entre les protocoles de courriel POP et IMAP . . . . . 104
Les vulnérabilités de l'e-mail . . . . . 105
Comment choisir votre fournisseur de mail ? . . . . . 108
Les webmails commerciaux . . . . . 108
Solutions d'e-mail alternatives . . . . . 109
Se protéger . . . . . 112
Adresse e-mail jetable : vers un e-mail propre . . . . . 114
Cryptographie et chiffrement . . . . . 116
Qu'est-ce que la cryptographie ? . . . . . 116
Comment la cryptographie protège-t-elle les messages ? . . . . 117
Vocabulaire de la cryptographie . . . . . 118
De quoi est constitué OpenPGP ? . . . . . 119
Le système de clef privée et de clef publique . . . . . 120
Générer sa clef . . . . . 121

Empreinte et signature . . . . . 122
Signer ses messages . . . . . 123
Chiffrer ses e-mails avec Enigmail . . . . . 124
Créer sa clef . . . . . 125
Envoyer la clef sur le serveur . . . . . 127
Stocker ses clefs . . . . . 128
Envoyer un message chiffré et signé . . . . . 128
Les problèmes posés par OpenPGP . . . . . 129
Le chiffrement ne suffit pas . . . . . 131
Messagerie instantanée . . . . . 132
Chiffrer vos discussions instantanées avec OTR . . . . . 135
Discuter en son et en images : la voix sur IP (VOIP) . . . . . 139
L'erreur humaine . . . . . 141

**7. Protéger sa connexion : proxies, VPN et le projet Tor . . . . . 143**

Les proxies . . . . . 143
Les proxies, comment ça marche ? . . . . . 144
Limitations du proxy . . . . . 144
Les proxies web, HTTP et SOCKS . . . . . 146
Comment utiliser un proxy ? . . . . . 147
Logiciels et extensions pour gérer les proxies . . . . . 149
Les réseaux privés virtuels ou VPN . . . . . 150
Qu'est-ce qu'un VPN et comment marche-t-il ? . . . . . 150
Points négatifs à l'utilisation d'un VPN . . . . . 151
Comment configure-t-on son VPN ? . . . . . 153
Comment choisir son VPN ? . . . . . 155
Tor, la solution la plus aboutie . . . . . 159
Comment Tor fonctionne-t-il ? . . . . . 160
Comment utiliser Tor ? . . . . . 161
Tor est-il vraiment sécurisé ? . . . . . 164
Autres réseaux anonymes . . . . . 164

**8. Sécuriser son smartphone et sa tablette . . 167**
Le contexte mobile . . . . . 167
Les faiblesses de votre téléphone . . . . . 168
Gérer les autorisations des applications . . . . . 170
Passer des appels chiffrés . . . . . 171
Sécuriser ses messages texte . . . . . 171
Solutions tout-en-un : tout faire avec un seul outil . . . . . 173
Naviguer de manière sécurisée. . . . . 173
Chats . . . . . 174
Utiliser un VPN avec son téléphone . . . . . 174
Remplacer son téléphone ou son système d'exploitation . . . . . 175
**9. Se protéger mieux et aller plus loin . . . . 177**
Protéger son mot de passe . . . . . 177
Vulnérabilité inhérente . . . . . 177
Les commandements du bon mot de passe . . . . . 178
Des logiciels pour stocker vos mots de passe . . . . . 180
Systèmes d'exploitation orientés sécurité . . . . . 181
Les fournisseurs d'accès à Internet (FAI) . . . . . 182
Payer en restant anonyme . . . . . 183
Aider ceux qui veulent être anonymes. . . . . 184
Aider les utilisateurs de Tor . . . . . 184
Donner de la bande passante… ou de l'argent ! . . . . . 186
S'informer et aller plus loin . . . . . 186
**10. Quel avenir pour l'anonymat ? . . . . . 189**
Des réformes s'annoncent . . . . . 190
Des pistes non étatiques . . . . . 191
La solution par les entreprises ? . . . . . 192
Vous avez dit démocratie ? . . . . . 194
Les effets néfastes de l'anonymat ? . . . . . 196
Le double jeu des politiques. . . . . 197
Renversement de paradigme . . . . . 198

**11. Entre la chaise et le clavier . . . . . 201**
Ne jamais faire confiance. . . . . 202
Comparer les coûts et les risques et s'adapter en fonction . . . . . 202
Internet n'est pas fait pour l'anonymat . . . . . 203
Comment choisir ses armes ? . . . . . 206
Choisir des outils utilisés par une large communauté d'utilisateurs . . . . . 206
Utiliser des logiciels libres . . . . . 208
Sélectionner une infrastructure décentralisée . . . . . 209
Méfiez-vous des entreprises. . . . . 210
Identifier votre « ennemi ». . . . . 211
L'erreur humaine et l'entraînement . . . . . 213
**Notes de fin . . . . . 215**
**Bibliographie . . . . . 227**
**Index . . . . . 231**

# Avant-propos

*L'anonymat sur Internet souffre d'un paradoxe étrange. Alors qu'on utilise de plus en plus Internet, qu'on y laisse toujours plus de données et qu'il est de plus en plus facile de savoir qui y fait quoi, l'inquiétude quant à l'utilisation de ces données grandit chaque jour.*

## Pourquoi ce livre ?

Jamais anonymat et vie privée n'ont été à ce point discutés et débattus. Et pour cause, sur Internet aujourd'hui, et plus spécifiquement pour les services les plus utilisés par le grand public, l'asymétrie d'information est totale.

D'un côté, les services gratuits proposés par les géants du Net offrent des avantages évidents et immédiatement perceptibles : gain de temps, facilité d'utilisation, innovations fréquentes. D'un autre côté, ces services fonctionnent pour l'essentiel grâce à nos données personnelles, collectées et agrégées de manière complètement opaque pour l'utilisa-

teur, rendant les dangers et les effets néfastes difficilement perceptibles.

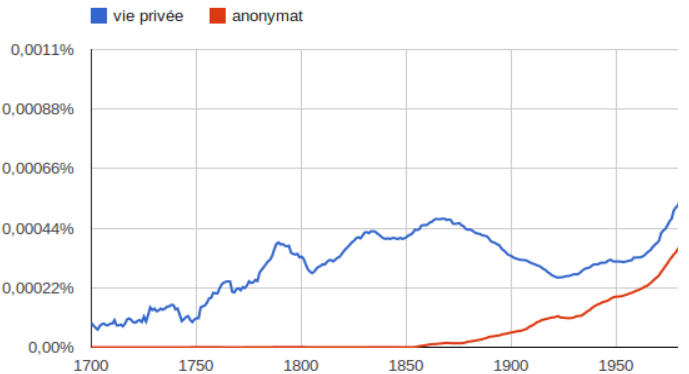



**Fig. 0–1 > L'évolution des termes « vie privée » et « anonymat » dans le corpus de livres indexés par Google**

Et pour cause : l'internaute non averti ne sait absolument pas quel type d'information personnelle il donne, quand il la donne, pour combien de temps, dans quel but ou pour quel profit, ni même, parfois, qui la collecte.

### Chiffres L'humanité, ou presque, sur Internet

**À l'heure où nous écrivons ces lignes, il y a 255 millions d'utilisateurs actifs sur Twitter[1], 1,3 milliard sur Facebook[2] et près de 200 millions de blogs[3] ; on n'a jamais autant parlé de soi sur Internet. Pour autant, la vie privée et l'anonymat n'ont jamais été aussi importants pour les internautes, à rebours d'un discours ambiant banalisant le naturisme numérique.**

Sur un réseau dont la mémoire et les capacités de copie sont en théorie illimitées, nul ne sait ce que nous prépare l'accumulation de données, traces et autres informations person-

nelles que nous laissons par térabits entiers, quotidiennement, sur Internet.

En savoir plus **L'hypermnésie**

Vous pouvez consulter à ce sujet la section consacrée à l'hypermnésie, du manuel *Informatique et sciences du numérique*.

📖 *Informatique et sciences du numérique*, Gilles Dowek *et al.*, Eyrolles, 2012

Une véritable option d'informatique a enfin fait son entrée au lycée, ce à quoi répond ce manuel adressé aux lycéens de Terminale S ayant choisi la spécialité ISN. C'est un manuel que chacun peut (et devrait) lire – en tout cas tout lecteur souhaitant comprendre les bases de l'informatique.

Cette question est cruciale et souvent dramatique pour les utilisateurs situés dans des pays intolérants, prompts à la surveillance, à la censure et à la répression.

Cependant, les citoyens occidentaux ont eux aussi matière à s'effrayer des velléités étatiques de contrôle et d'identification sur les réseaux. Les multiples révélations concernant les pratiques de la National Security Agency (NSA) ont été un réveil brutal pour ceux qui en doutaient encore.

Sans même aller jusqu'aux services de renseignement les mieux financés de la planète, les divers systèmes de traçabilité installés par les entreprises ou les particuliers et qui jalonnent nos existences numériques ont de quoi inquiéter nombre de citoyens.

Même si Internet est pensé et fait pour mener une vie publique, le glissement sur les réseaux de nos existences, de nos secrets et de notre intimité fournit de multiples raisons de protéger son anonymat et, de fait, son identité et sa vie privée.

Ce livre va tenter de vous donner une palette d'outils, de l'astuce la plus simple à la stratégie la plus complexe, pour

comprendre et protéger les informations que vous laissez filer à chacune de vos connexions.

DÉFINITIONS **Anonymat, vie privée, identité, sécurité…**

**Des thèmes connexes à l'anonymat seront évoqués et traités dans ce qui va suivre : vie privée, sécurité informatique… Il était difficile de faire autrement, tant ces domaines sont liés. Nous espérons, avec ce livre, faire un pont entre la théorie et la pratique, comprendre les mouvements en marche sur Internet pour mieux y adapter sa stratégie, comprendre le pourquoi pour appliquer le comment.**

Sur Internet, « on ne peut pas ne pas laisser de traces[4] ». Pourtant, ces outils sont nécessaires à ceux que cette bataille intéresse ou inquiète. Entre les grandes entreprises américaines qui tentent par tous les moyens de faire changer la perception de ce qui peut être privé et public sur le réseau, les efforts récurrents de certains acteurs étatiques pour contrôler ou « civiliser » Internet et les initiatives individuelles ou émanant d'entreprises qui se vantent de toujours davantage protéger la vie privée des internautes, les lignes de démarcation sont floues et mouvantes. Nous espérons modestement vous donner quelques points de repères au fil de ces pages.

Quant aux protections et aux outils que nous aborderons, ils sont parfois difficiles à comprendre et à appliquer : les menaces sur votre identité sont multiples et chacune présente ses caractéristiques propres. La sécurité est une question compliquée que l'on ne peut résoudre qu'en s'armant de temps, de patience et d'envie. Même si l'anonymat absolu n'existe pas, cela ne veut pas dire qu'il faut abandonner toute volonté de protection.

L'habitude est l'ennemie de la sécurité. Appliquer bêtement des processus et utiliser des logiciels sans comprendre leur fonctionnement peut tout autant vous mettre en danger que vous protéger. La sécurité informatique est un ensemble

cohérent où tout se tient. Les processus et les réflexes qui lui sont associés changent en permanence selon les évolutions technologiques, étatiques, juridiques ou commerciales. La sécurité n'est jamais acquise. C'est pour toutes ces raisons que ce livre ne donnera pas une liste exhaustive et définitive des moyens de protéger son anonymat et sa vie privée.

PÉREMPTION **La technique évolue (vite)**

**Dans le champ de la sécurité informatique, rien n'est jamais vraiment acquis. Certaines des solutions abordées dans cet ouvrage peuvent être obsolètes au moment de votre lecture, même si nous avons fait tout notre possible pour aborder uniquement des solutions éprouvées.**

# Plan de l'ouvrage

Après avoir défini un certain nombre de termes et rappelé quelques principes du fonctionnement d'Internet concernant l'anonymat (**chapitre 1**), on démontrera que l'anonymat total n'existe pas (**chapitre 2**). Pour autant, les raisons pour camoufler ses traces et son identité sont nombreuses (**chapitre 3**). Après avoir abordé les bases de la protection (**chapitre 4**), on se penchera sur les stratégies à mettre en place pour contourner la surveillance des entreprises et des géants du Web (**chapitre 5**). Puis on apprendra à protéger ses communications, notamment ses e-mails et ses discussions instantanées (**chapitre 6**), avant de se pencher sur la protection de sa connexion (**chapitre 7**), de son mobile et de sa tablette (**chapitre 8**) et d'aborder quelques outils plus techniques pour ceux qui désireraient aller plus loin (**chapitre 9**). Avant de dresser quelques pistes sur l'avenir de l'anonymat et de la vie privée sur Internet (**chapitre 11**), on abordera les réflexes fondamentaux à adopter sans même installer le moindre logiciel (**chapitre 10**).

# Remerciements

Cet ouvrage n'aurait jamais vu le jour sans le premier modem, arrivé dans la maison familiale à la fin des années 1990, et sans Muriel Shan Sei Fan et son e-mail de février 2012.

Je tiens également à remercier Chloé, qui aura supporté de m'entendre déblatérer pendant des mois sur la vie privée et la cryptographie en faisant mine de s'y intéresser (et pour le reste aussi). Il me faut également remercier l'équipe de Rue89, et plus particulièrement mes rédacteurs en chef, dont la confiance et la liberté qu'ils m'ont accordées sont pour beaucoup dans la réalisation de cet ouvrage, ainsi que les fidèles acolytes que sont Pirhoo, Mayeu et Pierre Alonso, pour leur aide et leurs relectures précieuses. Merci aussi aux tenanciers et piliers de bars de la mailing-list « AH » (ils se reconnaîtront) pour leur humour, leurs gifs animés et leurs sarcasmes, précieux alliés des derniers jours de rédaction. Les internautes qui ont gentiment répondu à mes questions sur les réseaux sociaux doivent aussi être remerciés ici, dont (j'en oublie) : @lactualaloupe, @_swayb, @nkgl, @barzin, @bmalynovytch, @zefede, @Zizounnette, @_LilyRUsh, @johanhufnagel ou encore @szadkowski_m. Enfin, sans les innombrables internautes, activistes, hackers et autres passionnés plus ou moins anonymes, qui ont passé du temps et de l'énergie à alimenter les ressources indispensables que sont wiki.korben.info, le site de l'EFF (www.eff.org), les diverses publications du collectif Tactical Tech, le Cryptoparty Handbook (www.cryptoparty.in/documentation/handbook), cet ouvrage ne serait pas ce qu'il est. Merci à eux.

# 1 Anonymat sur Internet : de quoi parle-t-on ?

*L'anonymat sur Internet est une notion qui revient fréquemment dans les débats et l'actualité, mais qui est souvent mal comprise. Commençons par quelques définitions.*

## Bien définir l'anonymat

On notera d'abord le caractère ambigu de l'anonymat : d'un côté, c'est ce qui est sans nom, sans valeur, parfois menaçant ou inexistant[5]. De l'autre, c'est une stratégie de protection, de préservation, porteuse d'égalité (dans le cas, par exemple, de l'anonymat du vote en France). Cette dualité se retrouve également sur Internet.

De ce constat que nous étayerons, on peut déduire plusieurs éléments caractéristiques de l'anonymat sur Internet qu'il est incontournable d'avoir en tête.

## Un anonymat tout relatif

Prenons comme exemple un scénario fictif : si je crée un compte Twitter, que je le dote d'un nom d'utilisateur aléatoire, que je conserve la photo de profil par défaut et que je ne poste aucune information permettant de m'identifier de quelque manière que ce soit (et sans prendre de précaution supplémentaire), je serai anonyme pour la majorité des utilisateurs de Twitter.

Mais pas pour mon fournisseur d'accès, qui saura dire – par exemple à la police – que je me suis connecté depuis mon abonnement Internet à twitter.com pour créer ce compte. Je ne serai pas non plus anonyme pour mon ou ma conjoint(e) qui consultera mon historique de navigation une fois que j'aurai quitté mon ordinateur.

On parlera donc de l'anonymat comme d'un état relatif (je suis anonyme pour mes collègues de travail, l'auteur d'un billet que je commente, l'hébergeur d'un site web…) dépendant de l'ensemble des précautions éventuellement prises.

Cet anonymat va dépendre à la fois des caractéristiques techniques du site ou du service concerné (stocke-t-il des données de connexion ? Requiert-il une adresse courriel valide ?), du contexte légal (les forces de l'ordre peuvent-elles contraindre ce service à divulguer mes informations ?), des outils déployés par l'internaute et, bien sûr, de ce qu'il va publier…

## Sur Internet, l'anonymat ne cache qu'une partie de son identité

Dans certains cas, remonter à un nom civil réel ne suffit pas (il y a bon nombre de Pierre Martin ou de Claude Duval en France). Parallèlement, un certain nombre de données qu'on pourrait considérer comme anodines peuvent être très révélatrices de l'identité d'un individu connecté. On pourra citer par exemple des commentaires sur des sites d'info, des goûts musicaux ou encore des requêtes sur un moteur de recherche.

## Neutralité (morale) de l'anonymat

C'est une évidence (qu'il serait tout de même bon de rappeler à certains hommes politiques), mais l'anonymat n'est pas bon ou mauvais en soi. C'est un outil qui peut être utilisé pour de bonnes ou de mauvaises actions, comme une voiture qui permet à la police d'arriver plus rapidement sur les lieux du braquage et aux bandits d'en fuir au plus vite.

# Définition de la vie privée

Anonymat et vie privée sont très souvent associés, et pour cause. Le premier est un moyen de préserver la seconde. La vie privée est la raison pour laquelle on peut vouloir recourir à des techniques d'anonymisation. Internet bouleverse la manière dont nous gérons notre vie privée et il est fondamental de le comprendre avant de prendre toute mesure pour protéger cette dernière.

## La vie privée, une nécessité selon Montaigne

C'est Aristote qui, le premier, donne une définition de la vie privée : il sépare la vie publique, celle de la cité, de la vie fami-

liale. Plus tard, Montaigne approfondit cette définition de manière très novatrice pour l'époque[6]. Selon lui, on ne peut être libre que s'il est possible de s'isoler du monde. Pour Montaigne, les opinions et la réflexion ne peuvent être formées librement que dans la sphère privée.

> 🕮 *Traitement des données personnelles*, Fabrice Mattatia, Eyrolles, 2013
> **Ce livre est un guide juridique sur les droits et obligations autour du traitement des données personnelles – utile à l'heure où la jurisprudence est parfois floue et mouvante. Aussi bien pour les particuliers qui veulent connaître leurs droits que pour les entités qui exploitent leurs données personnelles.**

La première définition moderne de la vie privée est donnée par deux juristes américains, Samuel Warren et Louis Brandeis, en 1890, dans un article de la *Harvard Law Review* intitulé « Le droit à la vie privée ». Selon eux, la vie privée se décompose en trois parties : le secret, la quiétude et l'autonomie. Ces trois dimensions se retrouvent de manière frappante dans le contexte numérique.

Le secret doit être entendu comme la « capacité d'un individu à contrôler la collecte et l'utilisation de ses données personnelles » ou la possibilité de choisir quand « ses attitudes, croyances et comportements et opinions doivent être partagés avec ou cachés des autres[7] ».

La quiétude consiste à pouvoir « se ménager une zone de quiétude en s'isolant de la société pour ne pas être ennuyé par […] l'intrusion des autres » ainsi que par « le contrôle de l'accessibilité à soi[8] ». Ce n'est donc pas seulement une notion d'espace ; elle recouvre également le champ des relations et de la communication. Certains auteurs font la différence entre la vie privée physique, informationnelle (ne pas être observé) et « attentionnelle » (ne pas être sollicité sans son accord)[9].

L'autonomie, enfin, découle d'une confusion fréquente lorsque l'on parle de vie privée : privé ne veut pas dire secret ! C'est aussi ce qui nous définit en propre en tant qu'individu, à savoir « son identité, ses opinions et sa manière de vivre[10] ».

Dans le monde numérique, ces définitions théoriques gardent toute leur pertinence.

## La vie privée numérique, c'est le contrôle

Pour Danah Boyd[11], la vie privée ne peut se comprendre qu'en termes de contrôle de ce qu'on laisse sur Internet : « La vie privée n'est pas une technologie binaire que l'on peut allumer ou éteindre. La vie privée renvoie au fait de pouvoir contrôler la situation, d'être en mesure de surveiller quelle information va où, et d'avoir la possibilité d'en réajuster le flux de manière appropriée lorsque l'information déborde ou va trop loin. Les gens se préoccupent de leur vie privée parce qu'ils ont peur d'en perdre le contrôle[12]. »

Les chercheurs Avner Levin et Patricia Sanchez Abril[13] en donnent une définition similaire. Pour eux, la vie privée consiste à conserver le contrôle d'une information personnelle et ne pas la laisser sortir du cadre dans lequel elle a été rendue publique (un cercle d'amis ou de collègues par exemple).

Pour être encore plus précis, on dira que la vie privée est une notion relative, un cloisonnement : « la volonté plus ou moins forte de cloisonner les divers aspects de son existence que [l'internaute] est le seul à connaître en totalité[14] ».

## Problème : on n'a pas toujours le contrôle

Les chercheurs Alain Rallet et Fabrice Rochelandet[15] distinguent deux types d'identification, notamment sur les réseaux : la première est volontaire, impulsée par l'internaute qui dépose un certain nombre d'informations personnelles à

dessein. Ces dernières sont cloisonnées, maîtrisées, adaptées au public que veut cibler l'internaute.

La seconde, qui vient dans un second temps, concerne ce qui est retrouvé, recollé, recoupé, en mettant à mal ce cloisonnement voulu par l'internaute, par exemple si on compile et analyse l'historique de ses saisies dans un moteur de recherche. L'intrusion dans la vie privée se situe bien davantage dans ce regard extérieur, et non dans les agissements de l'internaute, qui sait ce qu'il fait et met en œuvre des stratégies pour que tout ce qu'il fait ne soit pas visible par tout le monde. Cette attaque contre la vie privée se situe donc notamment dans les traces laissées par l'internaute involontairement ou collectées à son insu. La menace vient davantage des tiers et des traces non intentionnelles : « des traces faibles, mais nombreuses et diversifiées, [qui] apportent une information sur l'individu de plus grande valeur que des traces fortes mais peu nombreuses et redondantes[16] ».

La vie privée, c'est donc être en mesure de décider qui a accès à quelle information, de cloisonner sa vie numérique en fonction de son (ou ses) interlocuteur(s). Problème : de nombreuses menaces pèsent sur les moyens de contrôler sa vie privée. Heureusement, il y a des outils pour restaurer l'anonymat d'un certain nombre de données et donc protéger sa vie privée.

# Pourquoi Internet chamboule tout ?

La question de la vie privée et de l'anonymat trouve une nouvelle jeunesse avec Internet, pour plusieurs raisons.

HISTOIRE **L'invention de l'imprimerie**

**C'est le passage d'une culture de l'oral à une culture de l'imprimé[17], dans le sillage de l'invention de l'imprimerie, qui a permis le développement de la notion d'anonymat du lecteur. Auparavant, l'oralité de la communication rendait incontournable le face à face et impossible l'anonymat de l'audience.**

## Internet berceau de la vie publique

On comprend mieux l'Internet d'aujourd'hui et la question de l'anonymat si, au lieu de présenter la question sous le prisme de la vie privée, on le fait sous l'angle de la vie publique : désormais, plus besoin d'avoir des relations ou un statut particulier pour prendre la parole dans l'espace public. Internet nous donne justement de formidables moyens de mener une vie publique. Pour la première fois dans l'histoire de l'humanité, n'importe qui peut prendre la parole et être – du moins en théorie – un personnage public.

## Un renversement : une vie publique par défaut, privée seulement parfois

De fait, notre vie numérique, à l'exact inverse de notre vie hors-ligne, est publique par défaut et privée par choix[18]. Ce changement est de taille : la vie privée est davantage l'exception que la règle et il faut mettre en place des stratégies complexes pour la protéger. C'est ainsi toute la logique derrière les *Privacy Enhancing Technologies* (PET, technologies renfor-

çant la vie privée) : nous sommes surveillés par défaut et il faut regagner des espaces de vie privée.

**Précision Classification des technologies protégeant la vie privée**

Trois catégories peuvent être définies parmi ces technologies : celles qui agissent en intermédiaire (proxy), celles qui permettent de formuler un consentement informé et celles qui permettent d'être intraçable. D'autres préfèrent voir ces technologies du point de vue du niveau auquel elles s'appliquent : l'homme, l'appareil, le message, le réseau[19].

Dans ce contexte, on comprend mieux que l'anonymat soit devenu une question centrale, ainsi que l'ampleur des difficultés pour ceux qui entendent se ménager des espaces de vie privée et d'anonymat. Sur Internet, une vie privée est possible, mais il faut s'en donner la peine.

**Question Oublier la vie privée ?**

Jeff Jarvis[20], universitaire et fin analyste des médias et de la presse estime qu'il faut cesser de parler de vie privée et se pencher sur la vie publique : « Je pense que nous devrions déplacer la discussion des dangers qui pèsent sur la vie privée vers celle des bénéfices qu'il y a à tirer de la vie publique. Le problème ce n'est pas la vie privée, mais le contrôle qu'on en a. Et je dois avoir le droit, et les moyens, de garder secrète la maladie [Jeff Jarvis écrit cela alors qu'il vient d'annoncer sa maladie] si j'en ai envie. »

## Traces involontaires et invisibles

Internet renouvelle également la question de l'anonymat parce qu'on n'y laisse pas seulement des traces volontairement et de manière visible. S'il existe bien des traces visibles, les plus évidentes (un commentaire sur un blog ou une photo sur les réseaux sociaux), les traces invisibles sont légion (l'adresse IP quand on se connecte à un site Internet, sa requête dans les archives d'un moteur de recherche).

Il y a aussi des traces intentionnelles, celles que l'internaute a bien conscience de laisser, et des traces non intentionnelles : des cookies placés dans son navigateur ou un tracker (petit programme présent sur les sites web qui enregistre certaines de vos activités à des fins publicitaires) présent sur un site de e-commerce (voir les chapitres 4 et 5).

Le changement se situe également dans l'élargissement du nombre de données personnelles potentiellement identifiantes : qui aurait pu penser que, recoupés, analysés, un « like » sur une vidéo YouTube, un commentaire sur un site d'info ou une photo prise sur un smartphone puissent en révéler beaucoup sur notre vie privée et donc notre identité ? Toutes nos vies (professionnelle, personnelle, familiale, amicale, secrète, publique…) ont basculé dans le numérique ; les conséquences sont donc gigantesques.

Nous ne serions pas exhaustifs si nous ne mentionnions pas le fait que les données personnelles et l'identité de l'internaute sont devenues des unités marchandes de base d'Internet. Aujourd'hui, des pans entiers de l'économie numérique reposent sur la collecte, l'analyse et l'utilisation de données personnelles en échange d'un service (voir le chapitre 2). Cette tendance est presque aussi ancienne que la publicité et Internet la pousse dans ses retranchements.

## Le pseudonymat

Nos définitions seraient incomplètes si on n'évoquait pas l'avatar le plus commun de l'anonymat sur Internet : le pseudonymat.

L'usage du pseudonyme est extrêmement répandu sur Internet. Il diffère de l'anonymat en ce qu'il n'est pas une inconnue totale : si l'identité réelle reste secrète, une véritable identité avec des attributs proches d'une personnalité réelle[21]

peut se construire si le pseudonyme est utilisé sur de nombreux sites. De même, contrairement au discours ambiant, utiliser un pseudonyme pour protéger son anonymat n'est pas un abandon de ses responsabilités. On peut être critiqué, corrigé, félicité, dénigré, contredit sur le long terme, même abrité derrière un pseudonyme[22].

Toutefois, si l'utilisateur reste relativement maître de son pseudonyme et des attributs qu'il lui attache, ce dernier ne joue que sur l'identité déclarée et ne change rien à la collecte de données personnelles à l'insu de l'utilisateur.

### Peu de choses **Identifiés grâce à leurs pseudos**

**Des chercheurs ont montré qu'il était possible de profiler des utilisateurs et de compiler un certain nombre d'informations à leur propos, rien qu'en se basant sur leurs pseudonymes utilisés sur les réseaux.**

> http://www.technologyreview.com/news/422715/how-your-username-may-betray-you/

L'anonymat sur Internet, toujours précaire et relatif, est un moyen de protéger sa vie privée, c'est-à-dire de cloisonner et maîtriser les informations que l'on met en ligne ou que l'on collecte sans qu'on en ait forcément conscience. Si la vie privée est avant tout un problème de contrôle, l'anonymat et les technologies qui s'y apparentent, sont sans doute les outils les plus efficaces pour la protéger, tout en se cachant ou en obscurcissant/détournant certains aspects de sa vie.

# 2 Sur Internet, l'anonymat n'existe pas

*« Sur Internet, personne ne sait que vous êtes un chien. » Cette caricature*[23]*, parue en 1993 dans le New Yorker, est la plus célèbre et la plus citée lorsqu'on parle d'Internet. Cependant, en l'espace de vingt ans, elle est devenue fausse : on n'a jamais été aussi peu anonyme sur le Web. Techniquement, économiquement, politiquement, l'anonymat sur Internet recule.*

## Une pression croissante de l'État

Depuis une quinzaine d'années, les initiatives de la part des gouvernements pour tenter de réguler et de contrôler Internet se sont multipliées.

Les innombrables révélations à propos de la NSA, à partir du mois de juin 2013, ont servi de tonitruant réveil à ceux qui en doutaient encore.

Il est difficile de résumer en quelques lignes l'étendue de ce que nous a appris Edward Snowden, ancien sous-traitant de la toute puissante agence de renseignement américaine, en confiant à des journalistes une montagne de documents secrets.

Désormais, on comprend mieux les objectifs et le fonctionnement de cette agence, dont le principal credo est l'interception et le stockage de tout ce qu'il est possible de récupérer sur Internet.

Grâce à Edward Snowden, nous en savons plus sur l'implantation stratégique de stations d'écoute de la NSA, notamment sur les câbles transatlantiques qui acheminent le gros des communications mondiales[24].

Il est désormais clair que l'agence américaine est déterminée à affaiblir, voire contourner les systèmes de protection des communications les plus utilisés sur Internet par des millions d'internautes[25].

L'étroite collaboration entre les principales entreprises du Web, par l'intermédiaire notamment du programme Prism, est apparue en pleine lumière[26].

Les capacités de captation et de stockage de l'activité de millions d'individus sur Internet, sur leurs comptes courriels ou leurs téléphones mobiles ont été détaillées dans des documents Snowden[27].

On a également appris que l'agence pénétrait les réseaux internes de Google et de Yahoo! afin de collecter des carnets d'adresses et des courriels par dizaines de millions, en dehors de tout cadre légal[28].

La NSA a aussi forcé l'entrée de dizaines de milliers de réseaux divers (entreprises, administrations...) pour en prendre le contrôle et les surveiller, parfois simplement à titre préventif[29].

Que ce soit le jeu en ligne World of Warcraft[30], le chat vidéo Yahoo![31] ou les millions de photos partagées chaque jour par des millions d'internautes[32], parfois même les échanges télé-

phoniques de toute une nation[33], rien n'échappe à la NSA ou à son équivalent britannique, le GCHQ (*Government Communications Headquarters*).

La France n'est pas en reste, puisque son service de renseignement extérieur, la DGSE (Direction Générale de la Sécurité Extérieure), a également à sa disposition un système d'interception massif d'Internet[34] et peut compter sur sa proximité avec l'opérateur Orange pour prendre la main sur toutes les connexions qui y transitent[35].

Au-delà des services de renseignement, ces dernières années, le législateur français a été particulièrement prolixe pour réguler Internet : LCEN (loi pour la confiance en l'économie numérique), DADVSI (loi relative aux droits d'auteur et droits voisins dans la société de l'information), LOPPSI 2 (loi d'orientation et de programmation pour la performance de la sécurité intérieure), Hadopi (loi Création et Internet de la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet) ou encore les lois antiterroristes qui accroissent la surveillance du réseau à la recherche de potentiels terroristes.

De l'autre côté de l'Atlantique, on peut citer le DMCA (*Digital Millennium Copyright Act*), SOPA (*Stop Online Piracy Act*), PIPA (*PROTECT IP Act*) ou CISPA (*Cyber Intelligence Sharing and Protection Act*). Quelques tentatives de régulation ont été menées à l'échelon mondial, notamment avec le traité ACTA (*Anti-Counterfeiting Trade Agreement*)…

Longtemps vu et vécu comme un espace à l'écart de l'État, Internet a depuis été largement rattrapé par les gouvernants.

## Pour contrôler, il faut savoir qui est qui et qui fait quoi

Cette pression croissante des gouvernements à des fins de contrôle, de régulation et de surveillance ne peut se faire qu'au

détriment de l'anonymat des utilisateurs d'Internet. C'est en tout cas une des nombreuses thèses de *Code*, l'ouvrage précurseur du juriste américain Lawrence Lessig, un des premiers livres de référence sur Internet, paru en 1999.

Lessig prend l'exemple de la Pennsylvanie. Si les autorités de cet État américain voulaient interdire l'accès des mineurs de moins de 18 ans à tous les contenus pornographiques présents sur la Toile, elles auraient besoin de trois choses : savoir si le contenu contrôlé est effectivement pornographique et déterminer si l'internaute qui y accède est un mineur et s'il demeure en Pennsylvanie. Ces deux derniers critères sont résolument incompatibles avec l'anonymat.

Internet est en effet très différent de l'espace « réel » : Lessig pointe avec malice que, même déguisé, on pourra facilement reconnaître un enfant qui se présente à l'entrée d'un sex-shop. Dans le cyberespace, les paquets de données qui sont échangés en disent a priori peu sur l'âge, le nom ou la localisation de la personne qui en est destinataire.

Pour s'assurer du bon fonctionnement des lois que l'on veut édicter sur les activités en ligne, il faut nécessairement savoir qui fait quoi. Ce contrôle d'Internet par l'État ne peut donc se faire qu'au détriment de l'anonymat.

## Un exemple français : la conservation des données de connexion

En France, l'antagonisme entre l'intervention étatique et l'anonymat trouve une illustration parfaite dans une série, amorcée au début des années 2000, de lois et de décrets visant à conserver ce qu'on appelle les données de connexion, ou « logs ».

EXPLICATION **Que sont les logs ?**

**Lorsqu'un internaute se connecte à un site Internet, son adresse IP – l'identifiant plus ou moins unique de sa connexion – laisse quasi systématiquement une trace sur le serveur du site sur lequel il se connecte. L'ensemble de ces traces constituent l'historique des connexions à un même serveur : on appelle cela des « logs », des traces de connexion. L'écrasante majorité des serveurs utilisés par les services Internet conservent ces logs par défaut, même s'ils sont plus ou moins détaillés et conservés sur les serveurs plus ou moins longtemps.**

La France adopte le 15 novembre 2001 la loi sur la sécurité quotidienne : son article 29[36] oblige les fournisseurs d'accès à Internet à conserver les logs des connexions de leurs abonnés[37]. Ses mesures, dont l'article 29, auraient dû arriver à expiration fin décembre 2003. C'était sans compter un amendement de la loi sur la sécurité intérieure du 21 janvier 2003, qui a pérennisé les mesures de conservation des logs et les a séparées du motif terroriste, leur raison d'être lors de l'adoption de la première loi. Ces mesures sont désormais présentes dans l'article 34-1 du code des postes et des communications électroniques[38].

TERRORISME **Internet, outil très utile… à la justice**

**Le magistrat antiterroriste Marc Trévidic reconnaît volontiers qu'Internet, loin de n'être qu'un repère de méchants anonymes, est un formidable moyen… pour identifier ceux qui veulent rester anonymes le plus longtemps possible[39] !**

À partir de 2004 et de la loi pour la confiance en l'économie numérique, la conservation des logs, qui devait être effectuée « uniquement » par les « opérateurs de télécommunications » (donc les fournisseurs d'accès à Internet) concerne également les hébergeurs. Il faut entendre par là tous les sites qui mettent à disposition du public un service de « stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature[40] » :

c'est-à-dire tous les sites d'informations, les services de vidéo type Dailymotion ou YouTube, Wikipédia… Il a fallu attendre le 1er mars 2012 pour que le décret en précisant les modalités paraisse au Journal officiel[41].

## Comment ça marche ?

Par exemple, si l'utilisateur A, abonné au fournisseur X d'accès à Internet et doté de l'adresse IP 123.4.5.67, dépose, modifie ou supprime un commentaire sous une vidéo postée sur le site Dailymotion, ce dernier devra garder pendant un an l'information suivante : « L'utilisateur correspondant à l'adresse IP 123.4.5.67 et au fournisseur d'accès à Internet X a laissé (supprimé, modifié) le commentaire suivant le 13 avril à 13 h 18. » Si besoin, la justice s'adressera à Dailymotion pour lui demander les logs correspondant au commentaire auquel elle s'intéresse. Les fournisseurs d'accès peuvent quant à eux faire le lien entre une adresse IP et une identité bien réelle, celle de leur abonné. La même chose est possible du côté du FAI (fournisseur d'accès à Internet).

### Paranoïa ? Stockage des données

Les coûts nécessaires au stockage des télécommunications d'une nation tout entière vont bientôt devenir abordables, selon une étude du très sérieux *think tank* Brookings. À titre d'exemple[42], stocker l'intégralité des images captées par les 500 000 caméras installées par le pouvoir chinois à Chongqin coûte aujourd'hui environ 300 millions de dollars ; trop cher. En 2020, ce coût sera divisé par 100, soit 25 centimes par habitant. Aux États-Unis, on sait depuis les révélations Snowden que la NSA est capable de stocker l'activité en ligne de millions d'internautes, et même de stocker les appels téléphoniques de pays entiers. Les États-Unis sont désormais capables de tout voir et de tout entendre de ce qui se passe sur le réseau… Des informaticiens allemands ont calculé l'espace qui serait nécessaire au stockage de tous les renseignements contenus dans le dernier centre de stockage conçu par la NSA. Le résultat donne le vertige : les armoires d'archives occuperaient l'intégralité d'un carré dont la diagonale serait une ligne reliant Paris au golfe d'Aden ![43]

# L'anonymat remis en question pour des intérêts économiques

Une autre pression, plus insidieuse par certains aspects, s'exerce sur l'anonymat. C'est celle que font peser les entreprises qui, depuis le milieu des années 1990, ont investi (sur) la Toile.

### Traces Êtes-vous dépendant d'une entreprise sur Internet?

Disposez-vous d'un abonnement Internet ? Avez-vous déjà payé en ligne ? Avez-vous fait une recherche sur Google ? Disposez-vous d'un compte e-mail ? Avez-vous déjà mis en ligne une photo ? Rejoint un réseau social ? Lu un e-book ? Si tel est le cas, alors il y a toute une série de données personnelles vous concernant qui circulent un peu partout sur Internet. Le site myshadow.org/trace-my-shadow permet de se rendre compte du nombre de traces et de données personnelles qu'on laisse un peu partout via les entreprises auxquelles on a recours. Sans protection, quelqu'un qui aurait la même vie numérique que l'auteur de ces lignes laisserait 78 types de traces numériques différentes !

Pendant de longues années, les entreprises n'avaient pas d'intérêt à se risquer sur un réseau où les coûts étaient mutualisés, où peu de données autres que du texte pouvaient être échangées et qui était réservé à ceux qui avaient accès à une entreprise ou une université raccordée à Internet. Les premiers fournisseurs d'accès à Internet commerciaux n'ont fait leur apparition en France qu'au début des années 1990. Avant cette époque, Internet était vierge de tout intérêt commercial.

### Commerce Les marchands ont été longtemps bannis d'Internet

La National Science Foundation américaine, qui gérait le *backbone* d'Internet jusqu'au milieu des années 1990 a littéralement interdit le commerce sur Internet jusqu'en 1995[44] !

Puis le « www », sa navigation simplifiée, l'augmentation progressive du débit et l'adhésion toujours plus large du grand public à cette technologie ont poussé les entreprises à s'intéresser de plus près à ce que l'on pouvait monétiser sur Internet, et à réfléchir à des modèles économiques compatibles avec la rupture que constituait ce réseau.

Télématique **La place du Minitel en France**

**En France en particulier, la situation est encore plus compliquée, sa scène « télématique » étant dominée par le Minitel, qui a su séduire nombre d'entreprises grâce à son système de tarification limpide et son caractère très contrôlé, vertical et centralisé.**

## Valeur des données personnelles pour les « e-commerçants »

C'est avec ce qu'on a appelé le « Web 2.0 » que la pression des entreprises sur l'anonymat des internautes a commencé à s'exercer. « 2.0 » : ce terme un peu galvaudé désigne l'ensemble des services qui permettent aux utilisateurs de produire eux-mêmes du contenu, que ce soit des outils de *blogging*, l'avatar le plus commun du Web 2.0, mais aussi les sites de partage de vidéo ou, dans un second temps, les réseaux sociaux.

Des pans entiers de l'économie numérique se sont formés autour de services comme Google ou Facebook. Dans le premier cas, la richesse du moteur de recherche a été créée en tirant parti de « la multitude[45] », à savoir en organisant les liens hypertextes laissés au gré des milliards de pages web par les utilisateurs. Toutefois, les géants du Web trouvent de plus en plus une grande partie de leur valeur – et de leurs revenus – dans l'organisation et l'exploitation d'une masse bien plus conséquente d'informations : les informations personnelles, celles que les utilisateurs disséminent un peu partout. Internet

devient une place de marché où on échange des services contre ses données personnelles.

Lorsque la majorité des échanges entre les internautes et le réseau se faisait au niveau du moteur de recherche, le modèle économique de Google, par exemple, était d'une simplicité redoutable : il lui suffisait d'afficher des publicités en fonction des recherches de l'internaute.

## Un modèle économique reposant sur votre identité…

Désormais, c'est plus complexe : les interactions et donc la richesse se font de plus en plus entre les internautes. On pourrait décrire très grossièrement ce modèle économique de la manière suivante : les services que les internautes utilisent doivent en savoir le maximum sur ces derniers, sur leur identité, leurs échanges avec leurs pairs, leurs goûts, leurs habitudes, afin de rendre le service le plus efficace possible et donc de se rendre indispensables. Le but est de vendre cette connaissance à des annonceurs : c'est la base de leur modèle économique.

### Portrait Le fameux portrait d'un anonyme du Tigre

**Le sujet des données personnelles laissées sur Internet est sans doute apparu pour la première fois avec fracas dans les médias lors de la publication, par la revue *Le Tigre*, du portrait de Marc L. Le journaliste avait reconstitué la vie d'un inconnu avec pour seule base ce qu'il avait trouvé à son propos sur le Web[46].**

En 2010, dans les commentaires du site Metafilter, l'utilisateur « blue_beetle » formule[47] ce qui résume bien les modèles économiques nés avec le Web 2.0 : « Si vous ne payez pas, vous n'êtes pas un client, vous êtes le produit que l'on vend. »

### Débat Produit, peut-être, mais pas dupe

Dire que si l'on ne paie pas un service, c'est qu'on en est le service ne doit pas être une excuse qui permette à une entreprise de faire ce qu'elle veut avec vos contributions ou vos données personnelles. Il ne faut pas oublier que c'est un échange et que l'on peut tout à fait estimer que la qualité d'un service « vaut » la cession de quelques données personnelles. Pour décider cela, il faut une certaine forme de transparence : savoir ce que l'entreprise fait de vos données personnelles et être capable de s'en protéger. Une formule alternative a été proposée : « Si vous ne savez pas comment une startup gagne de l'argent, c'est qu'elle ne le sait pas non plus[48]. »

## … donc hostile à l'anonymat et au pseudonymat

Ces services sont de fait très hostiles à l'anonymat ou au pseudonymat, qui sont autant d'obstacles sur le chemin de la connaissance de leurs utilisateurs. L'ancienne directrice du marketing de Facebook, Randi Zuckerberg (par ailleurs grande sœur de Mark, le fondateur) a jugé que l'on devrait « mettre fin à l'anonymat sur Internet[49] », en opposant l'argument classique : « Les gens se comportent bien mieux quand ils le font sous leur vrai nom. Je pense que les gens se cachent derrière l'anonymat et ont le sentiment qu'ils peuvent dire ce qu'ils veulent derrière des portes closes. »

### Amende Google puni par la Cnil

En 2014, Google France a été condamné par la Cnil à 150 000 € d'amende. L'autorité de protection des données personnelles lui a reproché de ne pas avoir suffisamment informé ses utilisateurs lors de la fusion de l'ensemble des politiques de confidentialité de ses services. Outre cette somme, dérisoire au regard du chiffre d'affaire colossal du géant américain, ce dernier a dû afficher une notification de sa condamnation sur sa page d'accueil… Ce qui a eu pour effet de rendre le site de la Cnil brièvement inaccessible suite à l'afflux de visiteurs[50].

Mark Zuckerberg, le fondateur, a lui aussi fait part de ses plus grandes réserves, considérant que la vie privée était une « notion dépassée », lors d'une interview en 2010[51].

Facebook, et jusqu'à récemment Google+, le réseau social de Google lancé au début de l'été 2011[52], réclament le vrai nom de l'internaute. Le premier, par exemple, explique dans sa foire aux questions[53] : « Facebook est une communauté dans laquelle les gens communiquent en exposant leur identité réelle. Nous demandons à chacun d'utiliser ses vrais prénom et nom de famille. Cela aide à garantir la sécurité de notre communauté. La sécurité de notre communauté est très importante à nos yeux. C'est pourquoi nous supprimons les comptes établis avec un faux nom dès que nous les repérons. »

## L'anonymat, un obstacle au modèle économique du Web

Au fond, c'est logique. Prenons le cas de Google dont la devise est « d'organiser toute l'information du monde ». Comment parvenir à cette fin si une part croissante des informations du monde – du moins sur le Web – se trouve dans les réseaux sociaux, et si ces derniers sont peuplés d'utilisateurs sous pseudonymes ?

Le journaliste américain Daniel Lyons, dans *Newsweek*[54] estime que « leur modèle commercial est en totalité fondé sur la notion de "monétisation" de notre intimité ».

Stratégie **Faire régresser la vie privée ?**

L'enjeu pour Facebook (et les autres) peut être analysé comme suit : ces entreprises ont intérêt à habituer les gens à avoir leur vie privée de moins en moins dissimulée et donc d'autant plus monétisable. Facebook, par exemple, entretient une culture du *opt-out* : une nouveauté dans les paramètres de confidentialité – allant quasi-systématiquement vers plus d'ouverture – est automatiquement activée. C'est à la charge des utilisateurs les plus conscients et les plus au fait de ces changements, loin d'être la majorité, de désactiver cette nouveauté. On peut voir ces accrocs à la vie privée comme autant de tentatives d'accoutumance à l'érosion de cette dernière. Dans les transactions qui enrichissent le Web d'aujourd'hui, l'identité de l'internaute est souvent la matière première échangée et transformée.

Beaucoup objecteront que ces réseaux sociaux ne sont pas des entreprises philanthropiques, qu'il serait absurde de leur reprocher des pratiques qui tendent à favoriser leur activité et que le meilleur moyen de se défendre consiste encore à les éviter. Cependant, il est important de prendre en compte cette dynamique, tant par le nombre d'utilisateurs que ces réseaux concernent, que parce que la perception sociale de l'anonymat – hors et à l'intérieur des réseaux – est susceptible d'être influencée par la pression de ces entreprises. On ne sait pas à long terme quels dégâts ce déluge de données pourra causer.

Point de vue **Méchant Facebook ?**

« Facebook change nos attentes. Ils définissent la norme en termes de contrôle que les utilisateurs ont sur leur identité en ligne. Ils ont fait bouger cette barre lentement mais sûrement dans une direction qu'ils peuvent appeler transparence mais que d'autres peuvent voir comme un manque de choix[55] », explique Christopher Poole, alias « moot », le créateur du site 4Chan, où tous les utilisateurs peuvent être anonymes. Certains sociologues valident ce point de vue ; ils qualifient ces entreprises qui tentent de faire bouger les valeurs de la société dans un sens favorable à leur rentabilité d'« entrepreneurs de morale ».

## Un dilemme insurmontable : communiquer ou laisser des traces ?

Louise Merzeau, maître de conférences en sciences de l'information et de la communication, pointe[56] le dilemme incontournable qui menace l'internaute soucieux de son anonymat ou de sa vie privée : « Désormais, le volume de traces non intentionnelles qu'il laisse sur les réseaux dépasse en effet la part délibérée de son identité. Désormais, non seulement on ne peut pas ne pas communiquer, mais on ne peut pas ne pas laisser de traces. »

Et le problème vient justement de ces traces que l'on laisse involontairement.

### Surveillance Big Brother, c'est dépassé

Bruce Schneier, expert mondialement renommé de la sécurité informatique[57] écrit : « Dans *1984*, la collecte de données était délibérée : aujourd'hui, elle n'est plus intentionnelle. Dans la société de l'information, nous générons manuellement de l'information. Dans le monde d'Orwell, les gens étaient naturellement anonymes. Nous, nous laissons des empreintes numériques partout. La police de 1984 était centralisée, aujourd'hui elle est décentralisée. Votre opérateur téléphonique sait à qui vous parlez, votre banque sait où vous faites vos courses. Votre FAI peut lire vos e-mails, votre téléphone mobile peut surveiller vos mouvements et votre supermarché peut scruter vos habitudes de consommation. Il n'y a aucune entité gouvernementale qui rassemble tout ça, mais il n'y a pas besoin. Il n'y a plus un Big Brother, mais plutôt des milliers de little brothers. »

# La menace des « trackers » publicitaires

La menace la plus importante concernant l'anonymat et la vie privée des internautes ne vient pas des réseaux sociaux ou d'une soi-disant propension des jeunes au naturisme numérique. On en parle peu, mais elle vient de l'industrie publicitaire.

Chaque jour, lorsque vous surfez sur Internet, plusieurs dizaines d'entreprises vous suivent, vous tracent, vous surveillent : elles savent où vous allez, ce que vous achetez, ce que vous consommez. Elles sont même capables d'estimer vos revenus, le nombre de vos enfants, votre métier et votre âge[58]. Ensuite, ces entreprises vendent ou utilisent ces données pour afficher de la publicité très ciblée (certaines utilisent même ces données personnelles pour faire varier le prix en fonction du client[59]).

Le *Wall Street Journal* enquête depuis trois ans sur cette nouvelle forme de surveillance. Un de ses articles donne un exemple[60] : un client potentiel envoie un message à une concession automobile, via le formulaire de contact de son site web. Avant d'envoyer ce message, il a effectué de nombreuses recherches sur Internet pour affiner son choix en matière de prix et de modèles. Au moment de l'envoi du message à la concession, son e-mail est repéré par une entreprise spécialisée qui fournit à la concession une liste des sites visités et un profil (modèles préférés, budget envisagé).

## Comment les entreprises font-elles pour vous surveiller ?

La recette de ces entreprises est simple : la quasi-totalité des sites Internet comportent ce qu'on appelle des « trackers », ou traceurs. Qu'ils prennent la forme de cookies, de cookies flash (voir le chapitre 4) ou de balises (des petits bouts de code informatique), ils sont capables de surveiller votre navigation.

Et cela donne froid dans le dos : « Nous ne connaissons jamais rien sur une personne donnée », confie John Nardone, le PDG de [x+1], une entreprise du secteur[61]. Et pour cause ! Des chercheurs ont montré qu'en 2010, 80 % des mille principaux sites Internet comportaient des traceurs[62]. Certains sites ont actuellement plusieurs centaines de ces mouchards installés[63].

COMMERCE **Une centaine d'entreprises dans le secteur**

**Le secteur des traceurs regroupe une centaine d'acteurs : des réseaux publicitaires, des courtiers en données personnelles ou des entreprises spécialisées dans le « tracking »[64].**

Ces données personnelles sont ensuite échangées sur des places de marché : l'entreprise Bluekai, qui fait l'intermédiaire entre les publicitaires et ces entreprises, vend 50 millions d'informations sur des internautes par jour[65].

## Où se cachent les mouchards ?

Comment ces mouchards se trouvent-ils partout sur Internet ? Parfois, les entreprises qui les ont conçus rémunèrent les éditeurs pour qu'ils les fassent figurer sur leurs pages, mais c'est parfois plus insidieux. Certains sont contenus dans des fonctionnalités ou des contenus fournis gratuitement aux sites (un diaporama photo par exemple). D'autres sont dissimulés dans des publicités.

Il est normal pour certains sites d'utiliser des cookies ou des technologies similaires. Néanmoins, le *Wall Street Journal* estime que deux tiers des cookies installés sur les sites (il a étudié les cinquante sites principaux aux États-Unis qui comptent pour 40 % des pages consultées par les Américains) l'étaient à des fins de traçage.

PUB **La pub ciblée, moins embêtante que la publicité classique ?**

**« Si une publicité est correctement ciblée, cela n'est plus de la pub, cela devient une information importante », explique David Moore, PDG de 24/7 Real Media, un réseau publicitaire[66].**

## Les données collectées par les trackers sont anonymisées : un mythe ?

Beaucoup de ces entreprises spécialisées dans les données personnelles utilisent des méthodes pour anonymiser les données qu'elles traitent pour leurs clients[67]. Pourtant on va le voir, l'anonymisation des données est bien souvent un mythe.

De plus, comme nous l'évoquions dans le premier chapitre, sur Internet, l'anonymat ne se limite pas au nom. Il existe des centaines d'autres marqueurs d'identité, que ces traceurs connaissent et peuvent exploiter sans même avoir à connaître notre véritable identité. Joe Turow, auteur d'un livre sur les pratiques publicitaires en ligne[68], l'explique : « Si une entreprise peut suivre votre comportement dans l'environnement numérique, un environnement qui inclut potentiellement votre téléphone mobile ou votre télévision, l'idée que vous êtes "anonyme" n'a plus de sens. Cela importe peu si votre nom est John Smith, Yesh Mispar ou 3211466. La persistance de vos informations personnelles va conduire les entreprises à agir en fonction de ce qu'elles savent, partagent à propos de vous, que vous le sachiez ou non. »

### Anonyme ? Bluekai

**Sur le site bluekai.com/registry, il est possible de vérifier si l'entreprise Bluekai dispose de données personnelles nous appartenant. La réponse peut être pour le moins amusante : « Nous n'avons aucune donnée anonyme vous concernant. »**

Pour l'instant, beaucoup ont la sensation que cette collecte de données va trop loin, qu'elle n'est pas maîtrisée et se distingue comme « bizarre ». On ne sait pas quelles conséquences cela va avoir, c'est un monde complètement différent. Pourtant, avec les progrès dans l'analyse des données et dans les capacités

des ordinateurs, il se pourrait que les conséquences deviennent bien réelles.

# Les données ne sont jamais anonymes

À ce stade, il est possible de se dire que, certes, des données personnelles me concernant sont présentes un peu partout, mais qu'elles sont souvent dépourvues de tout élément permettant de les rattacher à ma véritable identité. Et qu'elles sont de toute façon anonymisées.

Malheureusement, de nombreuses recherches ont montré à quel point l'anonymat pouvait être précaire, et combien les données que nous laissons dans le sillage de nos navigations peuvent révéler notre identité et notre personnalité.

## Des critiques de films peuvent révéler une identité

En 2006, l'entreprise Netflix, spécialisée dans le visionnage de films en streaming, publiait 10 millions de recommandations et commentaires sur sa plate-forme rédigés par près de 500 000 de ses clients. Son but, en proposant ce matériau brut, était de permettre aux développeurs du monde entier de mettre en place un système de recommandation plus performant que celui qui existait auparavant. Toutes les données identifiantes contenues dans ces textes avaient bien évidemment été anonymisées et remplacées par des nombres aléatoires.

Pourtant, cela n'a pas suffi. Deux chercheurs de l'université d'Austin au Texas sont parvenus à lever l'anonymat de plusieurs utilisateurs de la plate-forme[69], simplement en croisant les données (notes et appréciations) publiées par Netflix avec d'autres, publiques et non anonymisées, encore présentes sur un autre site (IMDB). Certains internautes, qui avaient laissé

des appréciations similaires sur ce site avec leur véritable identité ont pu avoir cette dernière, pourtant précautionneusement dissimulée, révélée par un simple croisement avec des données publiquement disponibles.

## Identification par des requêtes dans un moteur de recherche

En 2006 toujours, Yahoo! avait rendu publiques plusieurs millions de requêtes de son moteur de recherche[70], toujours à des fins d'amélioration et de recherche. Cela représentait tout de même plusieurs centaines de milliers d'utilisateurs et Yahoo! avait pris ses précautions en anonymisant leurs noms le cas échéant, en leur attribuant un identifiant unique.

Des journalistes ont pourtant réussi à identifier l'utilisateur 4417749 (Thelma Arnold, alors 62 ans), simplement en consultant ses recherches, qui contenaient une multitude d'informations identifiantes (sa ville, ses chiens, son âge, sa situation maritale, ses envies de voyage).

C'était en 2006, bien avant que les réseaux sociaux n'explosent réellement. Puisque les simples moteurs de recherche suffisent à nous faire donner des quantités impressionnantes de données potentiellement identifiantes, on ne peut qu'être saisi de vertige à l'idée des données laissées sur les réseaux sociaux.

Une chercheuse a prouvé la vulnérabilité de nos identités en ligne, en montrant que 87 % des Américains peuvent être identifiés nominativement avec seulement trois données[71] : date de naissance, code postal et sexe. Or, on trouve presque systématiquement ces données en ligne, que ce soit sur les réseaux sociaux, les sites d'achats en ligne, les blogs, les forums…

## Le dossier médical d'un gouverneur identifié

Quelques années auparavant, la même chercheuse – Latanya Sweeney, alors étudiante – avait frappé un grand coup[72] : afin d'optimiser leurs services et de mieux comprendre le comportement de leurs patients, les services de santé de l'État du Massachusetts avaient publié les données médicales relatives aux hospitalisations de tous les fonctionnaires de l'État, en anonymisant évidemment le tout, en particulier les numéros de sécurité sociale, les noms et les adresses précises. Latanya Sweeney est pourtant parvenue à retrouver le dossier hospitalier du gouverneur de l'État. Ne connaissant que la ville de résidence du gouverneur, elle n'a eu qu'à se procurer pour 20 dollars la liste des inscrits sur les listes électorales de la ville (qui contenait le nom, l'adresse, la date de naissance et le code postal). Le reste était un jeu d'enfant : seules 6 personnes dans toute la ville avait la même date de naissance, trois étaient des hommes et un seul vivait au bon code postal.

RECOUPEMENT **L'anonymat ne suffit pas**

**Des chercheurs ont montré qu'il était assez facile de lever l'anonymat (même dans le cas de comptes n'utilisant pas leurs vrais noms) sur les réseaux sociaux en croisant des données. Ainsi, ils ont réussi à identifier des comptes Twitter anonymes simplement en comparant leurs relations avec celles d'un autre réseau social, où moins d'utilisateurs sont anonymes, Flickr[73]. D'autres ont fait une expérience encore plus frappante : après avoir assemblé et compilé dans un unique corpus des milliers d'articles de blogs, ils ont construit un algorithme capable, à partir de quelques paragraphes de texte pris au hasard, de retrouver qui en était l'auteur, et ce avec jusqu'à 80 % d'exactitude[74].**

Les leçons à tirer de ces quelques exemples sont simples : l'anonymat n'existe vraiment pas. Les géants du Web, et notamment les moteurs de recherche, sont assis sur une mine d'or en termes d'informations personnelles. Ces exemples montrent également que nous livrons énormément de nos

vies intimes rien qu'en parcourant les moteurs de recherche. Tout simplement, des pans entiers de nos vies (personnelle, amicale, professionnelle) se déroulent désormais en ligne.

## Les informations publiées sur le Web nous font-elles courir à notre ruine ?

Cela fait dire à Paul Ohm, professeur de droit[75] :

« Pour quasiment chaque personne sur terre, il y a au moins un fait à son propos stocké sur un ordinateur ou dans une base de données qu'un adversaire peut utiliser pour du chantage, de la discrimination, du harcèlement ou de l'usurpation d'identité. Je veux parler de choses plus graves que du simple embarras ou de la gêne, mais de dommages réels et légaux. Cela peut être des informations à propos d'une conduite passée, de sa santé ou d'une honte familiale. Pour quasiment chacun d'entre nous, de fait, on peut imaginer une " base de données de ruine ", qui contient ces informations qui étaient jusqu'à présent disséminées au travers de dizaines de bases de données autour du monde, et ainsi déconnectées de notre identité réelle. La réidentification a formé la base de données de la ruine et en a donné l'accès à nos pires ennemis. »

On pourra mettre deux bémols importants à ce danger. S'il est vrai que l'on révèle beaucoup de sa vie sur les moteurs de recherche, toutes ces informations peuvent également être de fausses pistes. Ainsi, l'utilisatrice identifiée de Yahoo! a expliqué avoir fait de nombreuses recherches – notamment médicales – sur le moteur de recherche pour ses amis.

Par ailleurs, si toutes ces données existent, elles ne sont pas utilisées de la même façon : elles ne sont pas toutes mises à profit pour nous vendre de la publicité ciblée et toutes les bases de données les contenant n'ont pas été croisées. Pour le moment, les grandes entreprises du Web ne savent pas forcément extraire le sens de cette montagne de données. Néan-

moins, puisque les enjeux financiers sont colossaux, il ne faut pas trop escompter que cette ignorance dure longtemps. Et on voit bien que, même anonymisées et retraitées pour ne pas porter atteinte à la vie privée, les traces que l'on laisse sur Internet peuvent être très parlantes vis-à-vis de notre identité.

D'un espace de liberté et d'anonymat à ses débuts, Internet s'est transformé en un espace que les gouvernements et les entreprises ont investi en force ; cela est particulièrement visible quand on se penche sur le domaine de l'anonymat.

La marchandisation d'une part, les velléités toujours plus pressantes de contrôle étatique d'autre part malmènent l'anonymat sur les réseaux. On voit d'ailleurs mal comment ces deux dynamiques étroitement liées pourraient être annulées, à moins de se doter des outils adéquats.

# 3 De l'intérêt de l'anonymat

*Même si l'anonymat total est inatteignable, les raisons de s'en approcher et de protéger sa vie privée sont nombreuses, que l'on soit membre d'une minorité (politique, ethnique, sexuelle), que l'on craigne pour son emploi, que l'on cherche à se protéger contre les violences en ligne ou simplement que l'on soit réticent à ce que son identité soit liée à ses propos et à son activité en ligne pour (presque) toujours (même si, et on le verra, le simple fait de protéger sa vie privée se justifie de lui-même).*

**Liste Les raisons de vivre sous anonymat et pseudonymat**

Une blogueuse a initié en 2011, lors du lancement de Google+, un sondage à l'attention des utilisateurs dont les comptes avaient été supprimés parce qu'ils n'utilisaient pas leur véritable nom. Un certain nombre de raisons d'être anonyme (ou d'utiliser un pseudonyme) sont apparues : un professeur qui n'a pas envie que ses activités en ligne soient liées à son nom, un auteur sous pseudo, une victime de harcèlement, un fonctionnaire à qui on a interdit de parler en son nom propre, une personne qui utilise un pseudonyme depuis des années et qui est connue *via* ce nom par un grand nombre de personnes, un individu qui veut parler de ses différences sexuelles sans utiliser son véritable nom ou une femme de fonctionnaire qui ne veut pas que ses opinions exprimées en ligne aient un effet sur la carrière de son mari[76].

# L'anonymat, une histoire de contrôle

Il existe sur Internet ce que le juriste américain Lawrence Lessig appelle le paradoxe de la vie privée : on y fait tout un tas de choses, pas forcément répréhensibles ou honteuses. Pourtant, malgré cette publicisation de notre vie, on ne s'attend pas à ce que cela soit totalement public et exploité par certains acteurs.

Ce paradoxe peut être résolu en utilisant un élément de l'anonymat sur Internet qu'on a évoqué dans le premier chapitre : la vie privée, c'est le contrôle sur l'information que l'on choisit de mettre en ligne. La volonté de s'exposer n'est donc pas du tout incompatible avec celle de se protéger. Et l'anonymat est justement un des moyens pour renforcer ce contrôle.

## Être qui on veut

C'est par exemple l'avis d'Andrew Lewman, le directeur exécutif de Tor (voir le chapitre 7) : « La possibilité d'être anonyme est de plus en plus importante parce que cela donne du contrôle aux individus, cela les laisse être créatifs, leur permet

de déterminer leur identité et d'explorer ce qu'ils veulent faire ou de s'informer sur des choses qui ne sont pas nécessairement " eux " et qu'ils ne veulent pas voir liées à leur véritable nom à perpétuité[77]. »

Ce n'est ni plus ni moins que la volonté de séparer les opinions politiques de l'identité réelle qui régit en France, par exemple, l'anonymat du vote.

### Capital L'exposition n'est pas bénéfique pour tous

**Pour la chercheuse Danah Boyd, tout le monde ne tire pas les bénéfices d'une vie publique sur Internet : il faut disposer d'un certain capital, ce qui n'est pas le cas de tous les internautes. Être visible et public sur Internet peut désavantager certaines catégories d'usagers, les plus défavorisées socialement et économiquement[78].**

## Le pseudonymat

Le pseudonyme, sans être complètement assimilable à l'anonymat (voir le chapitre 1), est une force efficace pour se protéger contre un certain nombre de dangers. Là encore, c'est une question de contrôle. En effet, sur Internet comme dans la vie de tous les jours, on ne se comporte pas de la même manière selon le contenu de son message (politique, professionnel, personnel) et de l'audience (un blog, un réseau social, une mailing-list professionnelle). Le pseudo permet de prendre en compte le caractère pluriel de toute personnalité.

### Chiffres L'anonymat contre le harcèlement

**La moitié des jeunes gays et lesbiennes sont harcelés en ligne[79] tandis que sur les services de messageries instantanées, les utilisateurs utilisant des pseudos féminins reçoivent des messages violents ou malveillants à un rythme 25 % supérieur.**

# L'anonymat et la liberté

Les questions de l'anonymat et de la liberté d'expression sont très intimement mêlées. Dans de nombreux cas, les internautes ne prennent la parole que si leur véritable identité n'est pas immédiatement accessible. Sur Internet, cette liberté d'expression prend des dimensions tout à fait inédites : n'importe qui peut intervenir dans l'espace public. Cette nouveauté n'est possible que si une protection existe parallèlement, tout le monde ne pouvant pas se permettre d'intervenir de la sorte et en son nom propre.

## L'anonymat, nécessaire à la liberté d'expression ?

Ainsi la justice sud-coréenne a-t-elle estimé que l'anonymat et le pseudonymat étaient nécessaires à la liberté d'expression. Elle a également considéré qu'obliger les internautes à utiliser leur véritable identité sur le Web n'avait pas d'effets notables en matière de réduction des incivilités[80]. Dans la décision McIntyre v. Ohio, un des juges de la Cour suprême des États-Unis a expliqué que « l'anonymat facilit[ait] un échange d'idées riche, divers et vaste ».

### Justice Facebook attaqué en justice pour non-respect de l'anonymat ?

**Parfois, le législateur s'empare de la question de l'anonymat avec vigueur. Le land allemand du Schleswig-Holstein a menacé d'attaquer Facebook en justice fin 2012. La raison ? Le réseau social ne permet pas l'utilisation de pseudonymes, ce qui serait contraire à la loi allemande[81].**

L'anonymat est fortement lié à une conception plus large de la liberté, selon la juriste Estelle de Marco[82] : « Il s'agit du pouvoir d'entretenir des relations par voie de communication

électronique. Il s'agit également de pouvoir faire des choix culturels, ludiques ou de consommation en ligne, ou simplement de s'informer, de naviguer librement sur le réseau. Cette liberté comprend encore le pouvoir de s'anonymiser ou de s'identifier à l'une ou l'autre de ces occasions. »

**Lecture** **Le droit de lire anonymement**

**Selon Julie E. Cohen[83], juriste américaine, l'anonymat doit être protégé en raison du premier amendement. Pour elle, l'anonymat est « un élément de notre liberté individuelle » : les systèmes de traçabilité (sur Internet mais également dans les e-books, les e-mails ou autres) doivent donc respecter l'anonymat. Comme l'explique Lawrence Lessig[84], « si le code doit savoir tout ce que je fais, au moins ne doit-il pas savoir que c'est "moi" qu'il surveille. Je suis moins embêté s'il sait que 14AH342BD7 lit ceci ou cela que si ce numéro renvoie à mon nom ».**

## L'anonymat protégé par la justice

Aux États-Unis, on peut d'ailleurs légalement considérer « qu'il n'y a pas de liberté sans droit à l'anonymat[85] », notamment parce que ce droit peut être déduit du très puissant premier amendement de la Constitution américaine, qui protège la liberté d'expression. Pour certains experts, le droit à l'anonymat et à la vie privée est un « socle » pour d'autres libertés[86].

Le respect de l'intimité et de l'anonymat permet à l'internaute (et plus généralement à l'être humain) d'exprimer sa créativité, d'explorer de nouvelles idées de manière bien plus libre que lorsqu'il est contraint par les diverses normes de la société. C'est notamment pour cette raison qu'Internet a eu un grand succès.

De fait, les effets de l'interdiction de l'anonymat ou de la surveillance sont très importants. Pour Daniel J. Solove, professeur de droit reconnu comme un des experts mondiaux les plus renommés en matière de vie privée, la surveillance a un

effet négatif inhibiteur, même si elle concerne des activités tout à fait légales[87].

De plus, il n'est nul besoin d'une surveillance permanente pour que celle-ci ait un effet inhibiteur sur les individus : dans *1984*, de George Orwell, les protagonistes ne sont pas surveillés en permanence, mais ils peuvent l'être. C'est cette potentialité qui est mortifère pour les libertés.

Dans son livre *Nulle part où se cacher*, dédié aux révélations Snowden dont il est le principal dépositaire des documents, le journaliste Glenn Greenwald relate une expérience de psychologie sociale menée à l'université de Stanford dans les années 1975. Des chercheurs ont demandé à deux groupes d'individus de se prononcer sur la consommation de marijuana. Au premier groupe, ils précisent que leurs propos seront transmis à la police à des « fins de formation » ; au second, rien de particulier.

Les résultats sont éloquents : 44 % des membres du premier groupe ont défendu la légalisation de la consommation de marijuana, contre 77 % des membres du second.

Plus proche de nous, une récente étude de l'ONG Pen auprès de plus de 500 auteurs américains à propos des révélations sur la NSA a produit des résultats effrayants : un auteur sur six interrogés avait spécifiquement évité d'écrire ou de discuter de certains sujets, de peur qu'ils soient l'objet de surveillance[88].

On peut ainsi estimer que le traçage et la surveillance renversent la charge de la preuve en supposant que tout le monde est un suspect en puissance. La solution la moins risquée pour l'internaute revient donc à se conformer à la norme et à sans cesse prouver qu'il ne fait rien de répréhensible ou sortant de la norme.

Ce mécanisme a notamment été étudié par Michel Foucault dans son ouvrage *Surveiller et punir* : la surveillance ne renforce pas seulement le pouvoir des surveillants, mais fait intérioriser aux surveillés le comportement que l'on attend d'eux.

En ce sens, l'anonymat peut être vu comme une garantie de ne pas être tracé, par opposition à un Internet où on est potentiellement surveillé en permanence.

Californie **L'anonymat, constitutionnel ?**

**Une loi obligeant les délinquants sexuels à donner tous leurs identifiants utilisés sur Internet a été provisoirement suspendue pour inconstitutionnalité, plus particulièrement avec le premier amendement de la Constitution**[89].

# L'argument « Je n'ai rien à cacher »

Un argument fréquemment utilisé pour minorer l'importance de l'anonymat sur Internet, et plus généralement pour minimiser les risques de la surveillance sous toutes ses formes consiste à dire que ceux qui n'ont rien à cacher (au gouvernement, aux entreprises) n'ont rien à craindre ou que nos informations personnelles n'ont que peu de valeur. Daniel J. Solove a consacré une partie de son travail à réfuter cet argument.

## Un argument un peu absurde

Premièrement, on peut repousser cet argument par l'absurde : (presque) personne ne serait d'accord pour être filmé en permanence et en toute situation jusqu'à sa mort ou voir des photographies de lui (ou elle) nu(e) diffusées sans autorisation sur Internet. Moins extrême, sur Internet, dès lors que l'on a acheté en ligne ou échangé des e-mails personnels, on commence à avoir des choses à mettre en sécurité (un numéro de carte bancaire, des conversations privées, etc.). Bref, on a toujours, forcément, quelque chose à cacher. Comme le disait Alexandre Soljenitsyne : « Tout le monde est coupable de quelque chose ou a quelque chose à cacher. Il suffit juste de chercher suffisamment pour le trouver[90]. »

Un autre argument peut être d'ordre philosophique : dire que la surveillance n'est pas gênante quand on n'a rien à se reprocher, c'est prendre la démocratie à l'envers. On peut penser que c'est justement parce que l'on n'a rien à se reprocher qu'il est intolérable d'être surveillé !

Pourtant, ces arguments sont en fait insuffisants. Cela tient au fait que la vie privée est mal définie. L'argument du « je n'ai rien à cacher » sous-entend qu'il n'y a que deux catégories d'actions : publiques (qui peuvent être assumées partout et toujours) et privées. Comme on l'a vu précédemment, sur Internet, ce n'est pas vraiment le cas.

## Trois exemples pour le réfuter

Trois exemples peuvent aider à comprendre cet argumentaire.

Si je cède un certain nombre de mes données personnelles à Facebook, je ne suis pas pour autant d'accord pour qu'ils les vendent à n'importe qui plutôt que de faire l'intermédiaire avec les publicitaires comme c'est le cas aujourd'hui. Pourtant, s'ils le font un jour, cela constituera une grave violation de la vie privée. Dans ce cas, les données auront été fournies volontairement, publiquement, et n'auront pas été altérées. Le problème ne se situe donc pas dans le caractère public ou non de ces données mais dans leur utilisation, ici différente de la raison pour laquelle elles ont été fournies.

On peut considérer que nos données de navigation n'ont que peu d'intérêt et qu'il n'est pas très embêtant qu'elles soient surveillées par des entreprises (ou l'État). On peut penser que, prises et étudiées individuellement, ces habitudes de navigation ou de recherches peuvent être parfaitement assumées en public. Le problème avec cette logique est que les entreprises (et l'État) mettent de plus en plus en œuvre des technologies d'analyse, parfois prédictive, de données, capables de déterminer une information C à partir des données de navigation

A et B. Il est beaucoup plus difficile de juger si cette nouvelle information C, calculée et déduite, va être tout aussi facile à assumer que les données initiales. Les « scientifiques des données » sont d'ores et déjà à l'œuvre[91] : il est aujourd'hui possible de savoir si un(e) internaute est susceptible d'avoir une maladie grave, de tromper sa femme ou d'être enceinte ! Là encore, le problème n'est pas la donnée (des habitudes de navigation) qui est en cause, mais la façon dont elle est traitée.

### Futur L'essor des technologies prédictives

De nombreux « scientifiques des données », statisticiens et autres mathématiciens cherchent dans les entreprises à prédire le futur grâce aux données[92]. Dans dix ans, on peut imaginer que des entreprises analyseront en profondeur les profils de leurs candidats à l'embauche, à la recherche de sens cachés parmi les millions de données qui y auront été déposées[93].

Troisième exemple : une entreprise peut collecter mes données avec mon accord, afin de me fournir un service. Si soudainement elle ne me laisse plus y avoir accès ou corriger une erreur qui y figure, c'est un vrai problème lié aux données personnelles et à la vie privée. Ce problème est tellement important qu'il est un délit pénal en droit français. Pourtant, comme dans les deux précédents exemples, j'ai fourni sciemment mes données et cela ne me dérange pas qu'elles soient publiques, je veux juste pouvoir les consulter et les modifier.

### Futur Kafka ou Orwell ?

Pour Solove, la comparaison de l'Internet d'aujourd'hui, où toujours plus de données personnelles sont collectées, avec *1984* n'est pas bonne. Il vaut mieux se tourner vers *Le procès* de Kafka : on ne sait pas quelle donnée est collectée, comment et par qui elle est traitée, ni qui a le pouvoir. Si les données comportent des erreurs, il est le plus souvent impossible de les corriger, il n'y a pas de transparence.

Les exemples peuvent être déclinés à l'infini. Sur Internet, rien ne garantit qu'une information ne parvienne pas entre de mauvaises mains, ou que les normes sociales soient les mêmes dans dix ans, ou qu'il n'y ait pas un piratage causant une fuite de données, ou que l'entreprise dont vous tolérez la surveillance ne change pas ses règles du jeu. Le fait que sur Internet, tout soit copiable, distribuable, stockable, analysable et bien souvent hors de portée, a un effet direct : rien ne peut garantir que vos données personnelles, aujourd'hui tout à fait assumées, ne deviennent pas très embarrassantes. Et si, dans dix ans, des données de navigation étaient utilisées pour vous refuser un crédit ou une assurance ? Dans les trois exemples précédents, je n'ai rien à cacher, je ne cache rien, pourtant j'ai à craindre de l'action des entreprises ou des états sur ma vie privée, car la vie privée ce n'est pas seulement le secret, c'est aussi le contrôle. Autant de raisons d'utiliser des techniques renforçant son anonymat sur Internet.

DIFFICULTÉS **Impossible d'accéder à ses propres données**

Même si la notion de propriété de données personnelles (qui sont des données numériques, facilement copiables et transférables) a des limites (comme nous l'enseigne la bataille de l'industrie musicale pour ses droits d'auteur), un des principaux dangers pointés par Solove est l'impossibilité d'accéder aux données nous concernant, ainsi que l'inconnu quant à la manière dont elles sont collectées et utilisées. Ces dangers ressemblent beaucoup à ceux que l'on peut imputer aux traceurs (voir le chapitre 2).

## Les choses commencent à changer

Plusieurs signes indiquent que l'acceptation de la surveillance par la population montre des signes de fatigue. Du moins, ils prouvent un certain attachement à la valeur de la vie privée en ligne.

Une récente étude de l'université d'Oxford auprès d'un échantillon représentatif de la population britannique montre que « la vie privée en ligne est en réalité une norme sociale forte ». À rebours des idées reçues, ce sont les plus jeunes qui sont les plus susceptibles d'avoir pris des mesures pour protéger leur identité en ligne sur les réseaux sociaux, notamment en modifiant les paramètres de confidentialité, davantage que leurs aînés[94].

### Suspecte **Tenter de camoufler sa grossesse**

**Une femme, professeur de sociologie, a récemment essayé de dissimuler sa grossesse à Internet (et à tous les acteurs qui le peuple). Elle en a tiré deux enseignements. Premièrement, cela nécessite des efforts colossaux, comme utiliser des logiciels complexes ou renoncer à l'utilisation de Facebook. Deuxièmement, cela l'a rendue suspecte : elle a reçu un message de l'entreprise auprès de laquelle elle se fournissait en cartes prépayées (pour éviter de laisser des traces avec sa carte bancaire) l'avertissant qu'en raison de sa fréquence d'achat, son cas avait été signalé aux autorités[95].**

Aux États-Unis, l'institut Pew Research Center interroge les Américains sur les politiques de sécurité contre le terrorisme. Pour la première fois depuis sa création en 2004, cet indicateur montre que les Américains pensant que la politique antiterroriste ne va pas assez loin sont moins nombreux (47 % contre 35 %) que ceux qui pensent qu'elle a trop restreint les libertés[96].

## L'anonymat et le droit

La loi et le droit ont des choses à nous dire sur l'anonymat et montrent notamment qu'il est tout à fait justifié.

Concernant la France, les textes qui encadrent le droit d'être anonyme sont morcelés et la protection qu'ils confèrent est large mais floue[97].

Pour la Déclaration des droits de l'homme de 1789, on est autorisé à « faire tout ce qui ne nuit pas à autrui » (Article IV[98]) : la liberté d'être anonyme n'est pas exclue.

Même si aucun texte supranational ou de valeur constitutionnelle n'évoque explicitement l'anonymat, le Conseil constitutionnel a reconnu et consolidé à plusieurs reprises le droit à la vie privée. Une déclaration du Conseil de l'Europe, adoptée le 28 mai 2003, y fait nettement référence : « Afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées, les États membres devraient respecter la volonté des usagers d'Internet de ne pas révéler leur identité ».

De manière générale, l'anonymat fait partie des libertés subjectives, par défaut, qui ne figurent explicitement dans aucun texte mais qui sont tout de même protégées. On trouve davantage de matière dans le droit concernant la vie privée.

## Qu'est-ce que la vie privée ?

L'article 8[99] de la Convention européenne des droits de l'homme est plus direct : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »

L'est également l'article 12 de la Déclaration universelle des droits de l'homme : « 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. »

Les articles 226-1 à 226-7 du Code pénal y font également référence. Quant au fameux article 9 du Code civil, il est d'une clarté absolue : « Chacun a droit au respect de sa vie privée. »

Paradoxalement, le juge français a pourtant du mal à définir les contours de la vie privée. Pour Estelle de Marco[100], il en découle « une certaine insécurité juridique de la personne

physique dans la protection des informations de vie qui la concernent et dont les tiers peuvent prendre possession. »

## Des dispositions plus précises dans d'autres textes juridiques

D'autres dispositions, plus précises, peuvent être invoquées pour protéger la vie privée.

L'article 226-15 du Code pénal, portant sur le secret des correspondances, protège l'anonymat de deux personnes échangeant sur Internet. Cette protection est ici collatérale, indirecte. C'est parce que le contenu des correspondances est secret que les éventuelles identités ou informations personnelles qui pourraient s'y trouver sont protégées, et non ces informations en elles-mêmes.

Plus généralement, la loi Informatique et libertés de 1978 qui encadre le traitement et l'utilisation des données à caractère personnel, offre de nombreuses protections. Les articles 323-1 à 323-7 du Code pénal (créés par la loi Informatique et libertés) répriment les atteintes portées à un système de traitement de données (par exemple une base de données d'une entreprise comprenant des adresses et des noms de clients). Un Français peut par exemple – et en théorie – obtenir d'un service la suppression des données le concernant, ou s'opposer à leur traitement. Les Américains n'ont pas cette liberté : aux États-Unis, aucune loi ne prévoit de tel mécanisme.

Enfin, le code des postes et des communications électroniques apporte une couche supplémentaire de protection pour l'internaute anonyme en considérant comme personnels et privés :

- les données relatives au trafic, c'est-à-dire l'information selon laquelle un internaute s'est connecté à telle heure à tel site ;
- l'ordinateur ;

- les données relatives à la localisation de l'équipement de l'internaute ;
- le téléphone mobile.

## Vers un véritable droit à l'anonymat ?

Pour Estelle de Marco, le législateur empiète trop sur le droit à l'anonymat sur Internet : « Les limites apportées par le législateur au respect qui est dû sur Internet à l'anonymat ne semblent donc pas globalement toujours répondre au critère de nécessité par la Cour européenne des droits de l'Homme. »

Selon la juriste, il conviendrait de sanctifier un véritable droit à l'anonymat, qui, pour le moment, n'existe pas en tant que tel dans les textes.

E-MAILS **La justice à la traîne**

**Aux États-Unis, c'est seulement en 2010 qu'une Cour d'appel fédérale a pour la première fois confirmé que le quatrième amendement de la Constitution (qui protège contre les perquisitions non justifiées) s'appliquait également aux e-mails**[101].

## Le droit est parfois mal adapté

Le droit n'est pas forcément adapté parce qu'on ne pensait pas que certaines informations, comme des commentaires de films, pourraient devenir identifiantes pour un certain nombre de personnes.

Si, en France, les données personnelles sont bien protégées et le droit à l'anonymat assez nettement reconnu, Internet est mondial et nos données et nos connexions ne restent pas circonscrites à l'hexagone.

De plus, l'anonymat est parfois hors la loi : en effet, la loi pour la confiance dans l'économie numérique de 2004 punit plus

sévèrement un crime ou un délit lorsque ce dernier a été commis avec l'aide de techniques cryptographiques (article 132-79[102]), le double lorsque la peine initialement prévue comportait au plus trois ans de réclusion criminelle, par exemple. Le refus de fournir la clef de déchiffrement dans un tel cas, ainsi que dans le cas où cela aurait pu éviter la commission d'un crime ou d'un délit est fortement puni par la loi (article 434-15-2 du Code pénal[103]).

DYNAMIQUE **Pour certains, l'anonymat recule**

**Pour la chercheuse Louise Merzeau, le législateur ne va pas dans le sens d'une plus grande protection des individus et un renforcement du droit à l'anonymat, mais favorise les mesures sécuritaires, visant à davantage de contrôle d'Internet et donc d'identification des internautes, tout en laissant les grandes entreprises « organiser la circulation des données ».**

# Typologie des menaces

À chaque type de menace concernant votre anonymat correspond une technique, des outils et des réflexes pour s'en prémunir.

## Les entreprises

À partir du moment où vous utilisez un service proposé par une entreprise, il faut accepter de confier son identité ou ses données personnelles à une entité qui poursuit un intérêt commercial avant tout. Ce dernier peut être compatible avec l'anonymat, mais il peut ne pas l'être toujours, que cette entreprise fournisse une extension pour votre navigateur (voir le chapitre 5), un réseau social, un service d'e-mail ou une boutique en ligne. Par exemple, si on accède sans protection à un site web classique, ce dernier va conserver les logs, les

détails de chaque connexion. On n'a jamais la garantie totale et absolue de ce qui sera fait avec nos données personnelles, ni maintenant, ni dans le futur.

### Ignorance Asymétrie d'information

Il y a là une très forte asymétrie entre l'utilisateur qui fournit des données personnelles et le fournisseur de service : d'un côté, le premier récolte vos données, vous connaît très bien et sait parfaitement comment utiliser ces données, de l'autre il n'est pas possible de savoir pour l'utilisateur comment ces données sont utilisées. On peut prendre l'exemple de Facebook : chaque utilisateur ne rapporte que cinq dollars par an[104], mais ses photos, commentaires, discussions qu'il a eues sont extrêmement importants pour lui. Ce contraste est saisissant. Si l'utilisateur est serein par rapport à cette disproportion, tant mieux. Pour les autres, des outils existent.

Par ailleurs, de nombreuses menaces se terrent dans l'ombre : certaines applications pour smartphones peuvent avoir un accès très large à vos informations personnelles et les envoyer vers des serveurs à distance sans que vous en soyez nécessairement informés[105]. Et c'est sans parler des entreprises qui surveillent de près votre navigation grâce aux traceurs (voir le chapitre 2).

### Contrepoint Et si le « tracking » était une bonne chose ?

Globalement, les entreprises demandent de plus en plus d'informations personnelles, autant d'obstacles sur le chemin de l'anonymat. Certains défendent l'idée selon laquelle les utilisateurs[106] reçoivent des services et des produits de même valeur que les données personnelles qu'ils consentent à fournir et que cela fait partie, depuis plusieurs années, de l'économie du Web. Selon eux, les questions de vie privée peuvent être réglées en se dotant des outils adéquats si cet échange « données contre service » dérange. Ce n'est pas si différent d'un achat normal, où l'accord est similaire : je te rends service, tu me donnes de l'argent. Cela suppose cependant de savoir parfaitement quelles données sont collectées, comment, dans quel but et avec quel traitement. Une utopie.

## L'État et la police

Dans certains cas, l'adversaire de votre anonymat sera la police. En France, la police et la justice disposent d'un arsenal législatif et judiciaire conséquent (voir le chapitre 2), qui rend en pratique l'anonymat difficile à maintenir.

### Gênant Ce que les services de police trouvent sur les réseaux sociaux

Les services de renseignement américains ont mené une enquête sur les réseaux sociaux : ils sont parvenus à trouver des informations notables (pas seulement des informations personnelles, mais d'autres plus ennuyeuses comme de la consommation d'alcool par des mineurs ou des positions politiques extrêmes) sur les réseaux sociaux à propos de plus de la moitié des personnes étudiées[107].

Aux États-Unis, le FBI peut avoir très facilement accès au contenu intégral d'une boîte e-mail et, plus largement, à toute forme de communication électronique[108]. De plus, les données de connexion peuvent être obtenues par la police sans aval de la justice[109]. Il ne faut pas oublier que les services que vous utilisez dépendent pour la plupart de la loi américaine !

L'anonymat peut également servir à se protéger contre d'éventuelles velléités de l'État en matière de surveillance : « même dans les corps de l'État les plus estimables et les plus respectables, il y a des tentations, des faiblesses, des fragilités », explique ainsi Noël Chahid-Noura[110].

### Classement La France très mal classée

Selon le rapport *European Privacy and Human Rights* réalisé par l'ONG Privacy International, la France figure parmi les pays qui se distinguent par l'ampleur des « points noirs » de leur législation et de leurs pratiques en matière de surveillance des individus[111]. En 2012, la France était « sous surveillance » dans le classement des ennemis d'Internet, réalisé par l'ONG Reporters sans frontières.

On ajoutera qu'on ne se protège pas nécessairement de la police de son pays, mais de celle d'un autre, ou de la police qui chercherait à identifier ou compromettre un correspondant qui habiterait dans un pays moins accueillant et tolérant que le sien.

## Piratage et défaillances

Lorsque l'on confie ses données à une entreprise ou qu'on lui fait confiance pour protéger son anonymat, on n'est jamais à l'abri d'une défaillance technique ou de l'action d'un pirate. Qu'un individu externe à l'entreprise parvienne à compromettre les données hébergées au sein de cette dernière ou que le danger vienne de l'intérieur et que vos données soient interceptées et consultées, les chances de voir ses données personnelles répandues dans la nature sont conséquentes.

Le site Privacyrights a répertorié toutes les fuites de données compromettant des informations personnelles (privacyrights.org/data-breach) : il y en a eu plus de 3 500 depuis 2005, pour un total de plus de 600 millions de données différentes. Dès que vous mettez une information (ou que vous communiquez) sur Internet, quel que soit son niveau de protection, elle est vulnérable à une éventuelle attaque. On peut également évoquer les piratages par Wi-Fi ou ceux qui adviennent lorsqu'un ordinateur est laissé sans surveillance et sans mot de passe ou protégé par un mot de passe faible (voir le chapitre 9).

Selon une étude de l'institut de recherche américain Pew Research Center, un adulte sur cinq a fait l'objet d'un vol de données personnelles sur Internet. Ce nombre est en constante augmentation[112].

## Vos proches

Un des dangers les plus sous-estimés et les plus courants est la surveillance que son cercle proche peut exercer.

« Ce que les gens ne réalisent pas, c'est que pirater et espionner sont devenus chose banale il y a dix ans », explique Dan Kaminsky, un chercheur en sécurité informatique[113]. « Ils pensent que pirater, c'est difficile. Pendant ce temps, tout le monde lit les mails de tout le monde, les petites amies ceux des petits amis, les patrons ceux de leurs employés, parce que c'est devenu très facile à faire. »

# 4 Les bases de la protection

*Dans ce chapitre, nous allons mettre les mains dans le cambouis, en commençant par le plus évident et le plus simple, là où beaucoup peut être entrepris pour préserver son anonymat : le navigateur. Avant cela, nous allons voir (et faire) ce que font tous les experts en sécurité informatique : estimer les risques et choisir une réponse appropriée.*

## Identifier ses ennemis et estimer le risque

La sécurité informatique (et donc la protection de l'anonymat), c'est un peu comme traverser la rue hors des clous lorsqu'on est pressé[114] : on évalue la menace de se faire écraser en regardant les voitures qui arrivent, puis on compare ce risque au temps que l'on perdrait à se rendre au passage clouté le plus proche.

Si les voitures sont nombreuses et roulent très vite, le risque couru est très important, alors on fait quelques pas vers les bandes blanches. Si, au contraire, la route semble déserte et le risque de se faire écraser faible, on traverse la route.

Évidemment, sur Internet et en informatique en général, le choix est plus complexe. Cependant, le mécanisme mental qui doit guider les choix à faire est tout à fait courant.

Pour être plus précis, les experts en sécurité informatique distinguent quatre éléments, qu'ils utilisent pour prendre des décisions :

- Les actifs (*assets*) : ce terme désigne tout élément qui a de la valeur. Ici, c'est bien évidemment de l'information, et plus spécifiquement votre anonymat ou votre vie privée.
- Les menaces : ces dernières représentent tout ce qui peut arriver de dommageable à vos actifs (dans l'exemple précédent, la menace était de se faire rouler dessus par une voiture lancée à pleine vitesse).
- Le risque : c'est-à-dire la probabilité pour qu'une menace, visant un des six éléments que nous allons voir, soit mise à exécution.
- Les adversaires : ceux qui sont susceptibles de mettre une menace à exécution ; à chaque adversaire peut correspondre une solution différente (voir le chapitre 3).

## Les six menaces pour votre vie privée

Les menaces peuvent recouvrir six dimensions différentes.

- La confidentialité de vos informations personnelles : elle est protégée lorsque des tiers ne peuvent pas accéder à ces informations.
- Leur intégrité : la garantie que vos informations ou vos données personnelles ne sont pas modifiées ou altérées par des tiers sans votre consentement.

- Leur disponibilité : vos données personnelles restent disponibles pour que vous (ainsi que ceux qui sont éventuellement autorisés à les consulter) puissiez y avoir accès.
- Leur cohérence (*consistency*, en anglais) : cette catégorie s'applique moins aux informations personnelles qu'à l'informatique de manière générale. Si vos données sont cohérentes, cela veut dire qu'elles fonctionnent comme prévu.
- Le contrôle : vous pouvez gérer et choisir librement qui a accès à vos informations personnelles.
- La possibilité d'audit : pouvoir auditer ses informations personnelles permet tout simplement de vérifier et de certifier qu'elles sont en sécurité et n'ont pas été compromises.

Cette nomenclature est assez utile pour connaître les points forts et les points faibles d'une technologie anonymisante. En effet, ces dimensions sont complémentaires et les techniques que nous allons étudier ne les protègent pas toutes simultanément. Prenons le chiffrement d'un e-mail, par exemple : cela garantit la confidentialité, l'intégrité et l'audit de vos données personnelles, mais pas les autres dimensions.

## Différencier risque et menace

Il y a une grande différence entre les menaces et les risques. Une menace très importante pour la vie de centaines de personnes peut correspondre à un risque assez faible : un tsunami géant en France, par exemple. À l'inverse, une menace assez faible pour la vie des individus peut correspondre à un risque très important : se faire voler son vélo à Paris.

Être capable de faire ce calcul avec autre chose qu'un tsunami et un vélo est sans doute la partie la plus cruciale lorsque vous décidez de protéger votre anonymat. Tout dépend de ce que vous estimez être important : certaines personnes vont considérer que la confidentialité des e-mails est quelque chose de vital et voudront prendre toutes les précautions nécessaires

pour se protéger. D'autres internautes préféreront éviter la collecte d'informations par des entreprises à leur insu lors de leur navigation.

C'est pour cela que l'évaluation des risques tient une place importante dans cet ouvrage (voir les chapitres 2 et 3). Quand on choisit un outil ou une procédure de sécurité, il faut toujours évaluer la menace (et ses conséquences) et le risque de voir cette menace subvenir.

## Les cinq commandements de l'anonymat

À ce stade de la lecture, vous êtes presque prêts à mettre les mains dans le cambouis de l'anonymat. Mais avant de commencer à installer le moindre programme, il y a quelques réflexes et principes à garder toujours à l'esprit lorsqu'on choisit un logiciel ou que l'on utilise un service[115].

Il faut d'abord se demander jusqu'où on est prêt à aller pour se défendre et protéger son identité. Le niveau de protection dépend intimement du temps passé à apprendre à maîtriser des outils et à comprendre leur fonctionnement. Certaines des technologies présentées dans ce livre sont assez techniques et nécessitent de l'investissement (en temps et en neurones). Le degré de dissimulation (qui n'est, rappelez-vous, jamais absolu) dépend toujours de la quantité de temps et d'effort que l'on veut bien y mettre.

QUESTIONS **Faire le calcul risques, coûts, menaces**

Quelques exemples de questions qu'il peut être nécessaire de se poser : est-il nécessaire d'utiliser un *remailer*, ou chiffrer mes e-mails suffira-t-il ? Faut-il bloquer tous les scripts en permanence ou juger au cas par cas ? Supprimer mon historique de navigation suffira-t-il pour que mes collègues de bureau ne connaissent pas mes préférences politiques ?

**Informez-vous.** Que cela concerne les menaces qui pèsent sur vos logiciels ou vos informations, ou les outils que vous allez utiliser pour les protéger, votre sécurité et votre anonymat dépendront toujours de l'information et de la bonne connaissance que vous possédez.

Heureusement pour vous, Internet regorge d'informations concernant l'anonymat, la vie privée et les technologies qui les protègent. De plus, la technologie évolue très vite et certains des outils présentés ici seront peut-être devenus obsolètes entre-temps. Rendez-vous au chapitre 9 pour quelques suggestions de lecture.

**Soyez proactifs.** Quand vos e-mails se retrouvent en plein jour, quand votre patron vous pose des questions sur le site que vous avez consulté la veille ou quand une entreprise a construit un profil marketing détaillé à partir de vos habitudes de navigation et de consommation, il est très difficile de revenir en arrière. Nous avons tous une tendance à la procrastination concernant la protection de nos données personnelles, d'autant plus que les menaces en informatique sont difficiles à percevoir et leurs effets souvent fortement différés dans le temps.

Il faut donc anticiper les menaces et vous protéger même si vous n'avez pas, pour le moment, de perception nette des dommages que votre identité en ligne pourrait vous causer. Nous ne sommes qu'au début de cette collecte un peu folle de données personnelles et nul n'est vraiment sûr de ce qui pourra en résulter.

**Le lien le plus faible.** Le dicton « la chaîne n'est jamais plus forte que le plus faible de ses maillons » est plus que jamais d'actualité dans le contexte de la protection de l'anonymat. Il est facile de le comprendre à l'aide d'un exemple extrêmement banal : à quoi sert-il de fermer sa porte à double tour si on laisse sa fenêtre grande ouverte (vous pouvez remplacer la porte par chiffrer ses e-mails et la fenêtre par mot de passe) ? Il

faut donc concentrer ses efforts sur la partie la plus exposée de votre identité en ligne.

**Cherchez la simplicité.** Plus l'outil ou la procédure de protection est simple, plus vous allez l'utiliser souvent, plus vous allez être entraîné, plus vous allez être en sécurité.

C'est aussi simple que cela. Utiliser un logiciel complexe, c'est le meilleur moyen de mal l'utiliser et de se créer un sentiment très dangereux de fausse sécurité.

**Il n'y a pas de sécurité parfaite.** Répétons-le : l'anonymat n'existe pas et aucune des technologies détaillées dans ce livre ne prétend vous offrir l'obscurité la plus totale. Nous sommes (normalement) tous des humains et les humains font des erreurs.

# Être anonyme : se protéger d'une menace inconnue

Comme si ce n'était pas assez compliqué comme ça, l'anonymat sur Internet comporte des particularités qu'il est fondamental d'avoir à l'esprit.

Lorsque l'on cherche à protéger son anonymat, on est en asymétrie totale d'information. Dit autrement, on se protège contre une menace invisible, dont on connaît rarement l'étendue des capacités techniques, notamment quand il s'agit d'un État ou de la police. Cette incertitude pousse à parer au scénario le plus catastrophique, quitte à se surprotéger.

## L'anonymat dépend des autres

L'anonymat et le secret de son identité dépendent beaucoup de la personne avec laquelle on interagit. Prenons un exemple (voir le chapitre 6) : si vous optez pour un compte e-mail

Hushmail sécurisé et chiffré, et que vous correspondez avec un ami qui utilise un compte Gmail sans protection particulière, vos précautions auront des effets beaucoup plus limités (puisqu'un gouvernement ou celui qui cherche à vous compromettre pourra éventuellement avoir accès à vos messages *via* le compte de votre correspondant). Idem, si, par souci de confidentialité, vous décidez de ne plus utiliser le service e-mail de Google afin que l'entreprise n'ait plus accès à vos messages, il vous faudra également cesser de correspondre avec vos correspondants utilisant Gmail.

## Un échange, plusieurs vulnérabilités

Enfin, l'anonymat sur Internet comporte plusieurs couches, qui, même prises indépendamment, peuvent révéler beaucoup concernant l'utilisateur. On peut citer le contenu de la discussion, l'outil utilisé (si vous utilisez un logiciel d'anonymisation qui est populaire parmi une certaine frange de la population – les activistes, une nationalité… – et que cela peut être détecté, cela peut compromettre votre identité), la nature de la connexion (une connexion ou un échange chiffré attirera plus facilement l'attention), les extrémités de la transmission (le site visité ou les interlocuteurs avec lesquels vous échangez). Globalement, on peut simplifier la chose en disant qu'il y a d'un côté le contenu, que l'on peut rendre confidentiel, illisible, et le contenant, le contexte (qui communique avec qui, quand et comment), que l'on peut anonymiser.

Certaines méthodes de protection vont concerner un ou plusieurs des aspects précédents et en laisser d'autres démunis. De même, les « adversaires » que vous avez éventuellement à affronter (entreprises, États, conjoints…) ne vont pas nécessairement s'intéresser aux mêmes aspects. Le simple fait d'utiliser la cryptographie peut vous valoir, dans certains pays, des ennuis avec les forces de l'ordre.

ATTENTION **Les ordinateurs publics**

**Utiliser un ordinateur public (bibliothèque, cybercafé) se révèle parfois risqué : il peut y avoir des virus, quelqu'un peut regarder ce que vous y faites, votre activité peut être surveillée et vous ne pouvez la plupart du temps pas installer d'outils pour vous protéger. À l'inverse, cela présente aussi un intérêt : si vous créez un compte e-mail depuis un cybercafé dans lequel personne ne vous connaît et où vous n'avez pas vos habitudes, il sera plus difficile, ultérieurement, de vous identifier comme le créateur de ce compte, l'adresse IP étant celle d'un lieu public. Cette dimension ambivalente est quasi systématiquement présente dans les solutions de sécurité qui sont abordées dans ce livre.**

On pourra résumer ces différents aspects par le contexte (qui, quand, où, comment) d'une transmission et par son contenu. L'envoi d'un e-mail chiffré va laisser secret le contenu (le message) mais pas le contenant (on voit très clairement les deux interlocuteurs malgré le chiffrement) ou certaines autres informations (quand vous vous connectez à votre webmail, avec quel outil, où, à quelle fréquence…) qui sont autant de moyens susceptibles de vous identifier[116].

L'anonymat est un assemblage d'outils, de techniques, de précautions, d'habitudes et de réflexes, qui ne peut pas être atteint simplement en plaquant des logiciels et des solutions « toutes faites ».

## Les questions à se poser

Si vous décidez, à la lecture de ce livre, de mettre en place un certain nombre d'outils et de procédures pour protéger votre vie privée, voici quelques questions (non exhaustives) que vous pouvez vous poser pour commencer.

- Avec qui vais-je échanger ? Quel site vais-je consulter ?
- Mon interlocuteur (ou le site) dispose-t-il (elle) des moyens de se (me) protéger ?
- Quelle information concernant mon interlocuteur ou moi-même ai-je besoin ou envie de protéger ? Est-ce que je veux simplement en empêcher la consultation ? La collecte ? L'altération ?

- Où se trouvent ces données ?
- De qui ai-je besoin ou envie de me protéger ? Qui est mon adversaire, mon surveillant ?
- De quelle(s) arme(s) mon adversaire dispose-t-il ? Quelle est la probabilité qu'il mette sa menace à exécution ?
- Quelles sont les « armes » dont je dispose ? Quelles sont leurs avantages et leurs inconvénients ? Leurs forces, leurs faiblesses ?
- Faut-il que je change d'outils ou que j'adopte un comportement différent en conséquence ? Mes « armes » sont-elles adaptées ?

Une autre possibilité, si vous souhaitez adopter une stratégie globale de protection de votre anonymat, consiste à faire une liste de tous les services que vous utilisez sur Internet (e-commerce, courriels, messagerie instantanée, réseaux sociaux, navigateur) susceptibles de détenir des informations personnelles et qui pourraient compromettre votre anonymat, auxquels vous ferez correspondre une série de menaces (interception, collecte d'informations à votre insu…).

Classez-les par ordre d'importance de la menace, puis par ordre de probabilité. Les éléments qui ont un risque élevé et constituent une menace importante doivent être traités en priorité. Ensuite, pour chaque item, il faut déterminer quels outils utiliser, leurs effets, leurs limites et les risques qu'ils posent.

### Réflexes Quelques précautions supplémentaires

**Pour ajouter un niveau de protection, on peut éventuellement créer des sessions d'utilisateurs séparées sur son ordinateur et utiliser uniquement celle sans pouvoir d'administrateur (ce qui limite la portée des failles de sécurité). Il convient également de protéger l'accès à sa session à l'aide d'un bon mot de passe (voir le chapitre 9). Les hackers les plus sensibles à leur vie privée et à la confidentialité de leurs données refusent d'utiliser leur ordinateur s'ils l'ont quitté des yeux ne serait-ce que quelques instants. Si vous courez un gros risque, ne laissez jamais votre matériel sans surveillance (une simple clef USB peut introduire quantité de saletés en quelques secondes).**

# Le navigateur

Pour afficher une page web, on ne se connecte pas directement au site en une seule fois. C'est un long chemin qui utilise de nombreux ordinateurs, lesquels se situent dans différents pays, sous différentes juridictions et appartiennent à des acteurs très différents (entreprises, universités…). De serveur en serveur, les informations que vous consultez (et/ou que vous envoyez) sont copiées, renvoyées et parfois stockées. Ainsi, l'interrogation d'une quinzaine de serveurs est nécessaire pour accéder au site d'Eyrolles, la maison d'édition de cet ouvrage, depuis un ordinateur situé en France.

Pour mieux comprendre, il faut rapidement se pencher sur le fonctionnement d'Internet.

## Naviguer, qu'est-ce que c'est ?

Internet, c'est un réseau d'ordinateurs connectés entre eux. Certains contiennent des documents qui, lorsqu'ils sont ouverts par des navigateurs, affichent des images, du texte, etc. Lorsque vous chargez votre navigateur d'afficher une page web, ce dernier va interroger le serveur sur lequel se trouve cette page. Pour ce faire, il va d'abord se connecter à un serveur DNS, une sorte d'annuaire des pages web. En effet, votre navigateur ne sait pas accéder à une page web dont l'adresse est du type : adressedelapage.fr.

Il va donc demander au serveur DNS à quelle adresse IP se situe le site.

VOCABULAIRE **L'adresse IP**

L'adresse IP est l'équivalent de l'adresse postale du serveur : chaque appareil connecté à Internet en possède une, y compris vous – elle vous est affectée par votre fournisseur d'accès à Internet.

Il va ensuite naviguer entre les ordinateurs (serveurs) qui constituent Internet – parfois près d'une vingtaine – et arrivera finalement au site demandé. Une connexion va être établie avec un des ports de ce serveur (l'équivalent des portes d'entrée du serveur, certaines étant plus « confidentielles » que d'autres, nous y reviendrons). Ce dernier va renvoyer sous forme de paquets (qui, à leur tour, vont emprunter jusqu'à une vingtaine de serveurs différents) un certain nombre de pages de code (HTML pour le contenu, CSS et JavaScript pour la façon dont ce contenu sera affiché) qui seront interprétées par le navigateur.

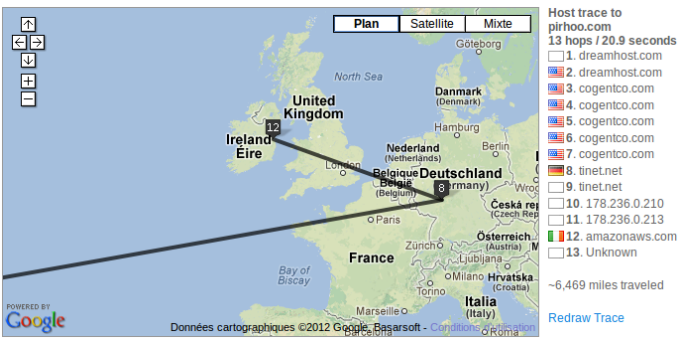



**Fig. 4–1 > Listes des serveurs utilisés pour accéder à un site Internet. Les pays indiqués peuvent différer de celui dans lequel est situé le serveur cible.**

Sans aucune précaution, un grand nombre d'informations (le navigateur utilisé, l'adresse IP, la localisation approximative, d'éventuels contenus de formulaire, la configuration de l'ordinateur, la page de destination, la page précédente, entre autres informations identifiantes) ont circulé en clair, c'est-à-dire sans protection, sur tous les serveurs interrogés.

En plus de ce mouvement d'allées et venues, de nombreuses informations transitent entre votre navigateur et Internet. Votre navigateur va sauvegarder votre historique de navigation, stocker des cookies, vérifier des mises à jour et communiquer avec bon nombre de serveurs en fonction de sa confi-

guration. Il laissera donc de nombreuses traces, à la fois sur votre navigateur et ailleurs sur Internet.

On se concentrera donc d'abord sur le navigateur, qui est le premier (sinon le seul) contact qu'un grand nombre d'utilisateurs ont avec Internet.

## Quel navigateur choisir ?

À des fins de protection de la vie privée, on optera pour un navigateur libre plutôt que pour un navigateur propriétaire (voir le chapitre 10). On ne saurait trop conseiller le navigateur de la fondation Mozilla, le très célèbre Firefox. Il a l'avantage de comporter un très grand nombre d'extensions, dont beaucoup sont utiles à la protection de l'anonymat. Il existe des navigateurs de qualité propriétaires comme Chrome (Google), Safari (Apple) ou Opéra.

### Histoire **Origines et succès de Firefox**

Créé en 2003, ce navigateur libre et gratuit a constitué la première vraie concurrence pour l'Internet Explorer de Microsoft et représente aujourd'hui environ 20 % de part de marché des navigateurs[117]. Il est traduit en 89 langues[118]. Ses extensions (de petits programmes qui s'installent dans le navigateur pour y apporter des fonctionnalités supplémentaires) sont sa plus grande richesse : 100 millions d'entre elles ont été téléchargées en 2012. Il peut être installé en se rendant sur la page suivante :

> mozilla.org/fr/firefox/

On pourra éventuellement choisir Chromium, la déclinaison open source du navigateur Chrome, réputé pour sa vitesse. Les extensions disponibles pour Chrome sont également disponibles pour Chromium, même si la compatibilité n'est pas toujours parfaite.

DÉBAT **Chromium, vraiment à recommander ?**

**Chromium est effectivement distribué avec une licence open source et reprend la quasi-totalité du code source de Chrome. Il communique cependant avec les serveurs de Google[119]. Nous recommandons Firefox, mais certains ne peuvent se passer de Chrome.**

Pour faire plus simple, nous parlerons ainsi principalement de Firefox et Chrome. Certaines des extensions et fonctionnalités présentées sont également disponibles sur d'autres navigateurs.

## Pourquoi importe-t-il de protéger son navigateur ?

Le navigateur est le point d'entrée principal vers le Web. En l'absence de toute forme de protection, on peut considérer[120] que tout ce que vous faites dans ce navigateur, autrement dit votre activité sur le réseau, peut être enregistré, sur votre machine ou sur n'importe quel serveur avec lequel vous communiquez.

Par défaut, votre navigateur collecte beaucoup d'informations susceptibles de vous identifier[121].

On peut citer notamment des copies des pages visitées, des informations concernant les noms d'utilisateurs et les mots de passe que vous utilisez, des données que vous avez insérées dans des formulaires, des cookies, votre historique de recherche, etc.

Ces informations sont stockées localement sur votre ordinateur et sont accessibles à quiconque ayant accès à votre machine.

Les navigateurs en eux-mêmes sont bavards. Si vous optez pour une solution propriétaire, le navigateur est susceptible de transmettre à des entreprises des informations personnelles. Ce n'est pas le cas de Firefox.

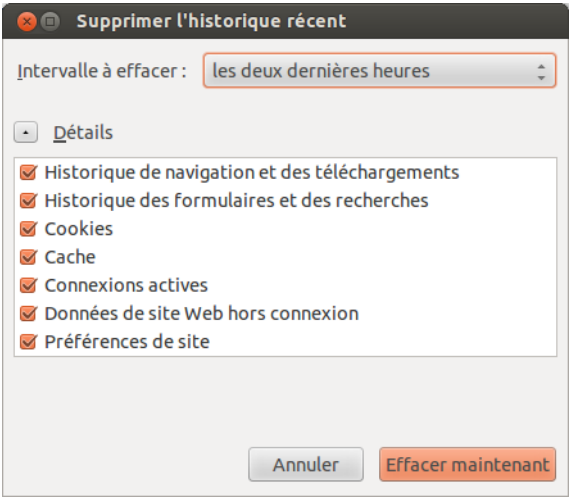



FIG. 4–2 > Accessible grâce à un raccourci clavier, ce menu permet de voir les types d'informations retenus par Firefox.

### FUITES Les informations que Chrome envoie à Google

Chrome, lorsqu'il est paramétré par défaut, communique beaucoup avec Google et laisse nombre de vos informations personnelles lui parvenir. Par exemple, lorsque vous tapez une recherche dans la barre d'utilisation, votre adresse IP et certains cookies parviennent à Google. On notera cependant un notable effort de transparence de la part de l'entreprise californienne, qui mentionne ainsi le délai dans lequel les éventuelles informations personnelles collectées (historique des recherches par exemple) sont supprimées (plusieurs semaines). Enfin, Chrome peut être paramétré d'une manière assez similaire à celle de Firefox, que nous allons évoquer, pour protéger votre vie privée.

Pour prendre la mesure du nombre d'informations qu'un navigateur configuré par défaut laisse filtrer, il suffit de se rendre sur le site panopticlick.eff.org. Développé par l'ONG de défense des libertés sur Internet Electronic Frontier Founda-

tion, il permet un diagnostic des informations transmises par votre navigateur. On citera pêle-mêle : la page précédemment consultée, la version de votre navigateur, votre système d'exploitation, votre langue ou les extensions (ou jeux !) installées sur votre navigateur.

Cela peut sembler dérisoire et sans grande conséquence. panopticlick.eff.org est doté d'une autre fonctionnalité : il indique si la configuration et les caractéristiques de notre navigateur sont uniques parmi les 2,6 millions de tests qu'il a réalisés jusqu'à présent. Dans le cas de l'auteur (qui utilisait, à des fins de test, une configuration tout à fait banale), ses caractéristiques étaient totalement uniques, comme c'est le cas pour 86 % des navigateurs[122] !

PRÉCISION **Des bits d'information très parlants**

**Selon la théorie dite de l'entropie, il suffit de 33 bits d'information pour identifier nommément une personne. Ainsi, le jour et le mois de la naissance d'un individu, ainsi que son code postal, nous donnent aux États-Unis 32 bits d'entropie. Il suffit de connaître son sexe pour arriver au seuil des 33 bits d'entropie. Le site https://panopticlick.eff.org nous apprend par exemple qu'un navigateur laisse passer autour d'une vingtaine de bits d'entropie[123].**

## Ne pas laisser de traces avec son navigateur

Heureusement, de nombreuses astuces existent pour limiter les traces que nous laissons au fil de notre navigation.

Il convient déjà de mettre à jour très fréquemment son navigateur, idéalement dès qu'on nous le propose. Des failles de sécurité sont en effet fréquemment découvertes et des logiciels à jour limitent les risques.

Fin 2012, Firefox a intégré la fonctionnalité *Do Not Track* (voir le chapitre 3), qui indique aux sites que vous visitez (et aux petits bouts de sites tiers) que vous ne désirez pas être pisté.

Cette fonctionnalité est facilement activable dans l'onglet *Vie privée* des paramètres de Firefox. Chrome, Safari et Internet Explorer disposent eux aussi de cette option.

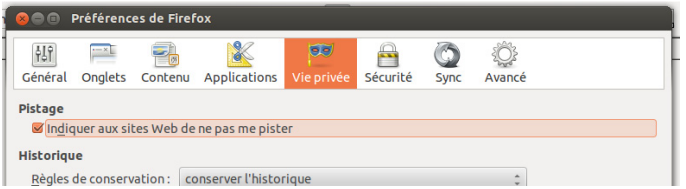



FIG. 4–3 > Accessible dans les paramètres du navigateur, cette option est très facile à activer.

Malheureusement, de nombreux sites ne respectent pas ce nouveau standard et ne tiennent aucun compte de ce paramètre.

Dans l'onglet *Avancé/Réseau* des paramètres de Firefox, il est également possible de limiter la part de la mémoire de votre ordinateur allouée au cache du navigateur, là où ce dernier stocke un certain nombre de données hors connexion. Cela peut rendre la navigation sur certains sites légèrement plus lente.

Les navigateurs, par défaut, vous proposent de stocker les mots de passe pour ne pas avoir à les saisir systématiquement. Si cette fonctionnalité est extrêmement pratique, elle permet à quiconque ayant accès à votre ordinateur d'accéder facilement à tous vos comptes. Le risque est grand de voir vos comptes et toutes les informations personnelles qui y sont attachées compromis. Reportez-vous au chapitre 9 pour bien choisir votre mot de passe. Il est toujours possible, depuis les paramètres du navigateur, d'en désactiver la mémorisation.

## Désactiver ou supprimer l'historique de navigation

Par défaut, votre navigateur enregistre dans son historique toutes les pages que vous consultez. Cela peut s'avérer problématique si quelqu'un d'autre que vous a accès à votre ordina-

teur (ordinateur familial, partagé dans l'entreprise, ordinateur de bibliothèque ou de cybercafé). Votre historique peut être extrêmement révélateur de vos goûts, de vos intérêts politiques, professionnels, de vos projets, vos inquiétudes, votre santé… Bref, de votre identité !

Heureusement, il est très facile de supprimer l'historique ou de désactiver sa mémorisation par votre navigateur, ici Firefox.

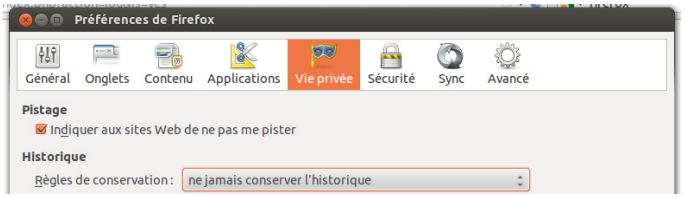



FIG. 4–4 > Comment désactiver la mémorisation par défaut de votre historique de navigation

Plus important que les œillades indiscrètes de votre conjoint(e) ou de votre voisin de bibliothèque, il est possible pour un site web de récupérer la liste des sites que vous avez visités[124] !

## Mode navigation privée

Un des premiers outils qui vient à l'esprit de beaucoup lorsqu'on parle d'anonymat sur Internet est la navigation privée, une fonctionnalité désormais présente dans la quasi-totalité des navigateurs grand public. Avant toute chose, il faut savoir que cette fonctionnalité n'a pas vocation à vous rendre complètement anonyme : les sites consultés ou votre fournisseur d'accès peuvent encore vous pister, ou accéder à votre adresse IP.

Elle a en revanche plusieurs fonctionnalités intéressantes. Lorsque vous passez en mode navigation privée sur Firefox, plusieurs types de données ne sont plus enregistrés[125] : les pages visitées, les données saisies dans les formulaires et la

barre de recherche, les mots de passe, la liste des téléchargements, les cookies, les fichiers temporaires. Afin de maximiser la protection de l'anonymat, les fonctionnalités de ce type de navigation devraient être la règle plutôt que l'exception.

L'activation de la navigation privée s'effectue par le raccourci clavier *CTRL+MAJ+P* ou le menu *Outil* pour Firefox et par le raccourci *MAJ+CTRL+N* ou le menu *Options* (clef) pour Chrome. L'activation de la navigation privée se manifeste généralement par un léger changement de couleur des menus du navigateur et par l'apparition d'une petite icône (un masque de carnaval pour Firefox, un homme masqué pour Chrome).

Cette fonctionnalité donne un anonymat assez correct, uniquement du côté navigateur, lorsque vous utilisez par exemple un ordinateur public.

L'extension *Ghost incognito* pour Chrome[126] automatise la navigation incognito sur certains sites que vous définissez.

LIMITES **Les défauts de la navigation privée**

Des chercheurs de Stanford ont mené une étude sur les systèmes de navigation privée[127]. Outre le fait que cette fonctionnalité est davantage utilisée par les amateurs de pornographie que par les internautes soucieux de leur vie privée (sans doute parce que c'est une solution assez peu avancée), les chercheurs ont montré deux problèmes avec la navigation privée. Le premier, c'est que sur certains navigateurs, lorsque la connexion est effectuée en SSL, le certificat produit par le site visité reste sur l'ordinateur, preuve de la visite de ce site pour un éventuel œil extérieur. Deuxième problème : sur Firefox, plusieurs extensions ont une compatibilité limitée avec le mode navigation privée.

## Cookies

Parmi les informations stockées par votre navigateur et qui peuvent être utilisées par de sites tiers, les cookies ont une place particulière.

### Définition Qu'est-ce qu'un cookie ?

Les cookies sont de petits fichiers stockés sur votre ordinateur. Ils lient toutes vos activités sur un même site. Chaque fois que vous retournez sur le site qui l'a créé, le cookie utilise les informations qu'il stocke : votre identifiant et votre mot de passe, votre ville de résidence… Tout ceci dépend du type de site que vous visitez. Cela permet par exemple de mémoriser un mot de passe ou de sauvegarder d'autres types de préférences. On distingue les cookies secondaires (déposés par le site que vous visitez) des cookies tiers (installés par des scripts ou des sites présents sur le site que vous visitez).

En effet, certains cookies sont utilisés pour voir comment vous interagissez avec un site. Dans le cas des cookies tiers, ils sont utilisés par un autre site que celui sur lequel vous l'avez obtenu (permettant ainsi de croiser vos données de navigation par exemple). C'est le cas de nombreuses régies publicitaires : les cookies qu'elles implantent servent de véritables fiches signalétiques de l'internaute.

### Miam Les « super cookies » Flash

La société Adobe, célèbre pour son logiciel Flash, a créé un type particulier de cookies, aussi appelés *local shared objects* (LSO). Ils sont particulièrement bien cachés et collectent de nombreuses informations personnelles. Heureusement, de nombreuses extensions pour les navigateurs existent pour les supprimer et Adobe fournit également quelques conseils[128].

Plusieurs paramètres peuvent être modifiés au sein de votre navigateur pour limiter ces effets négatifs. Tous les cookies ont une date d'expiration : on peut par exemple forcer la destruction de tous les cookies à la fermeture du navigateur, refuser tout stockage de cookies (mais cela risque de rendre certains sites inutilisables) ou paramétrer des règles personnalisées, autorisant les cookies uniquement sur certains sites de confiance.

### En pratique Gérer les cookies

Vous pouvez gérer les cookies manuellement en modifiant les paramètres des navigateurs.

- **Chrome :** *Paramètres > Paramètres avancés > Paramètre du contenu* ;
- **Firefox :** *Historique > Vie privée > Paramètres personnalisés* **ou** *Options > Vie privée > Supprimer des cookies spécifiques*.

Si vous autorisez le stockage de cookies par votre navigateur, il peut être judicieux de purger tous ses cookies (depuis les paramètres) à intervalles réguliers, afin de limiter les possibilités de pistage. On peut également n'autoriser que les cookies secondaires et interdire les cookies tiers.

Même si rien ne vaut une gestion « à la main », de nombreuses extensions pour Firefox et Chrome permettent de gérer les cookies, notamment *Cookie Manager Plus* pour Firefox.

### Attention Les dangers des extensions

Utiliser des extensions dans un navigateur pose plusieurs problèmes : cela peut ralentir votre navigateur, perturber le fonctionnement de certains sites ou poser des problèmes de compatibilité avec votre navigateur ou entre extensions. Enfin, toutes les extensions ne sont pas des logiciels libres et certaines peuvent être dangereuses. Le site addons.mozilla.org permet aux utilisateurs de noter les extensions proposées et de laisser des commentaires ; n'hésitez pas à les parcourir avant d'installer un nouveau programme sur votre ordinateur.

## « HTTPS everywhere »

Le protocole utilisé pour accéder aux pages web est appelé le HTTP. Sa principale faiblesse ? Rien n'empêche une oreille indiscrète sur le réseau de voir à quels sites vous accédez et leur contenu, et même éventuellement d'altérer ce protocole.

HTTPS (surnom de la technologie SSL) est le même protocole, mais chiffré (il accède à un serveur par le port 443, contre le port 80 pour le HTTP). Il permet trois choses :

- Le contenu de la page ne peut pas être vu.
- Le contenu de la page ne peut pas être modifié.
- La page que vous visitez vous a bien été adressée par le site dont l'adresse s'affiche dans la barre d'adresse (via un système de signatures cryptographiques vérifiées par des entreprises spécialisées).

Les habitués des sites de e-commerce ou des sites de banques connaissent bien cette technologie : un petit cadenas s'affiche, la couleur de la barre d'adresse change et un « s » s'ajoute au « http ».

### Faille L'histoire de « Heartbleed »

**En 2014, déjà éprouvé par les révélations sur la NSA, le monde de la sécurité informatique a été secoué par « Heartbleed », nom donné à une faille découverte dans OpenSSL, une bibliothèque chargée de mettre en œuvre le HTTPS sur une majorité de sites web de par le monde. Cette faille béante anéantissait toute forme de protection des communications de manière totalement furtive, permettant ainsi de dérober mots de passe, détail de la navigation, numéros de carte bancaire...[129] La plupart des sites sécurisant leurs données avec cette technologie ont été affectés. En France, la plupart des sites de e-commerce, les grands réseaux sociaux et même les banques ont été touchés. Encore aujourd'hui, le conseil donné après que ces services ont corrigé la faille demeure : il faut changer régulièrement son mot de passe (si cela n'a pas été fait).**

L'Electronic Frontier Foundation a développé une extension pour Chrome et Firefox, appelée *HTTPS everywhere*. Elle porte bien son nom puisque, une fois installée, elle « force » les sites visités à passer en HTTPS.

> eff.org/https-everywhere

Sa principale limite ? L'extension fonctionne en se basant sur une « liste blanche », une liste de sites (environ 1 500[130]) où l'extension va s'activer. On ne peut donc pas se connecter en HTTPS aux sites qui n'y figurent pas. Il est heureusement possible d'ajouter manuellement des sites.

De plus, si tous les sites où la confidentialité est absolument nécessaire (comme les sites de e-commerce) ont implémenté la technologie, tous ne la proposent pas : il faut en effet que le serveur soit compatible. De fait, lorsqu'on essaie de forcer la connexion (en ajoutant un « S » à « HTTP », par exemple) sur un serveur non compatible, ce dernier affiche une erreur (il est également impossible d'utiliser l'extension *HTTPS everywhere* sur ce type de site). La connexion repasse donc « en clair », c'est-à-dire non chiffrée et aux yeux de tous.


**Fig. 4–5 > Il est impossible de se connecter au site du Figaro de manière sécurisée !**

L'EFF a également réalisé une étude des pratiques de chiffrement des principaux services sur le Web, cherchant notamment s'ils activent le HTTPS ou s'ils mettent en œuvre un système de chiffrement plus performant, le « Forward secrecy » (où les connexions ne sont pas chiffrées – et donc déchiffrables – avec une seule clef maîtresse en possession du fournisseur de service, mais individuellement, avec des clefs différentes à chaque fois, accroissant de fait la protection).

Étude **Pratiques de chiffrement**

> https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what

Astuce **Passer en HTTPS manuellement**

Il est possible, en ajoutant un « S » au « HTTP » dans la barre d'adresse sur le site que vous visitez, de « forcer » la connexion en HTTPS (c'est ce que fait l'extension *HTTPS everywhere*). Votre navigateur affichera dans un premier temps un message d'avertissement : en effet, il ne parviendra pas à vérifier la signature cryptographique du site que vous essayez de visiter en HTTPS (et pour cause, si vous forcez le passage, c'est qu'il ne l'a pas prévu). Il faut ajouter une exception de sécurité pour continuer la navigation (à vos risques et périls, l'adresse du site pouvant avoir été usurpée).
Suite à la publication de documents par Edward Snowden détaillant les efforts de la NSA pour altérer et affaiblir les technologies de cryptographie grand public, les spéculations sont allées bon train : il semble très probable que l'agence américaine soit en mesure de « casser » le HTTPS[131].

## Les requêtes HTTP

Nous venons d'évoquer le protocole HTTP. À chaque fois que votre navigateur sollicite l'affichage d'une page, il fait ce qu'on appelle une requête HTTP. Cette dernière contient des informations potentiellement identifiantes, notamment la dernière page visitée ou le type de navigateur.

Plusieurs extensions existent pour contrôler ce qui est communiqué dans ces requêtes, notamment RefControl ; d'une part, ce dernier établit une liste de sites et définit ce qui doit figurer dans les requêtes HTTP pour chacun d'eux, d'autre part, il définit un comportement « par défaut » pour ceux qui ne figurent pas dans la liste.

Il est même possible de forcer Firefox à interdire les *referers* (c'est-à-dire l'information qui indique au site sur lequel vous vous rendez sur quelle page vous vous trouviez précédem-

ment), limitant le nombre d'informations envoyées par chaque requête HTTP. Pour cela, il faut saisir `about:config` dans la barre d'adresse, passer outre le message d'avertissement, taper `referer` dans le champ de recherche, cliquer-droit sur le résultat qui s'affiche, cliquer sur *Modifier* et remplacer le `1` qui s'affiche dans la barre de texte par un `0`.

**Débat Faut-il désactiver JavaScript ?**

**Le JavaScript est un langage qui permet à une page web de faire des calculs et des modifications sans que vous ayez à la recharger. Si quelqu'un arrive à introduire son propre programme JavaScript (appelé script) sur une page tierce, il peut s'en servir pour intercepter des informations sur les visiteurs, détourner des mots de passe ou altérer le contenu de la page.**

Il est possible de désactiver totalement le JavaScript depuis les paramètres du navigateur. De nombreuses extensions permettent de ne l'autoriser que sur certains sites de confiance, de voir tous les scripts de la page et de détecter les codes malveillants (voir au chapitre 5).

## L'adresse IP

L'adresse IP (Internet Protocol) est en quelque sorte l'adresse postale de votre connexion à Internet. C'est une des données les plus identifiantes que vous semez en ligne (votre fournisseur d'accès à Internet sait quel abonné se cache derrière une adresse IP donnée). On peut aussi la comparer à une carte de visite : la connaître, c'est savoir où vous êtes. Il peut donc être intéressant de la dissimuler. Il est possible de le faire directement depuis le navigateur, via un certain nombre d'extensions. Cependant, cette solution a de grandes limites : vous devez faire confiance à l'éditeur (parfois obscur) d'une extension pour gérer un bien aussi important que l'adresse IP ; il

faut s'assurer que les serveurs dudit éditeur ne gardent pas de trace de votre connexion, que personne ne vous espionne là-bas ou que le chemin (la connexion) est protégé (chiffré). On trouvera des moyens de se protéger, plus simples et plus efficaces, dans le chapitre 7.

On peut déjà utiliser une « recette de grand-mère », qui minimise les dégâts en termes de vie privée vis-à-vis des sites que vous visitez, mais pas de votre fournisseur d'accès : éteindre votre box ou votre modem à la fin de chaque session de navigation. Ainsi, votre fournisseur d'accès à Internet vous réattribue une nouvelle adresse IP à chaque connexion (cela ne brouillera votre identification que pour les sites visités, pas pour votre fournisseur d'accès). Attention, si vous disposez d'une adresse IP fixe, cela ne fonctionne pas. Si vous ne savez pas de quel type d'adresse IP vous disposez, cela veut très certainement dire que votre adresse n'est pas fixe.

Certaines extensions font transiter votre connexion via leurs serveurs. On citera IPFlood (ipflood.paulds.fr), Stealthy.co et surtout Privoxy.org. Ce dernier dispose de fonctionnalités intéressantes (altération des requêtes HTTP, filtrage des publicités) et il est libre !

## D'autres outils plus complexes pour dissimuler les traces du navigateur

D'autres outils sont disponibles pour brouiller vos traces. Presque anecdotique, l'extension *User agent switcher* permet de changer l'*user agent*, qui indique au site que vous visitez les versions de votre navigateur et de votre système d'exploitation.

Il est également possible de supprimer les entrées DNS cachées sur Windows. Ces archives des demandes que vous avez effectuées précédemment auprès de serveurs DNS (souvenez-vous, ces demandes servent à transformer un nom de domaine – trucmachin.fr – en adresse IP, à laquelle votre navigateur

peut accéder) sont stockées sur votre ordinateur et peuvent révéler l'historique de votre navigation, même si cette dernière a été effectuée en mode privé ou si vous ne sauvegardez pas votre historique. Pour supprimer ces entrées, il suffit de taper `ipconfig /flushdns` dans l'invite de commande de Windows (souvent via *Bureau > Exécuter*).

Dans Firefox, il existe un espace de stockage temporaire, qui peut contenir des informations sensibles. Pour le supprimer, il suffit de taper `about:config` dans la barre d'adresse puis `storage` dans le champ de recherche. Changez d'un clic-droit la valeur de `dom.storage.enabled` à `false`.

Pour faciliter l'élimination des nombreuses traces (historique, cookies…) que vous laissez derrière vous, on suggérera l'utilisation de l'extension *Close'n'Forget*, qui nettoiera derrière vous après chaque fermeture d'onglet. Il vous reste toujours la possibilité de supprimer, dans tout navigateur, les données enregistrées en pressant *CTRL + ALT + SUPPR*.

Vous voici désormais équipé pour utiliser un navigateur sans laisser la moindre trace sur votre machine. Toutefois, ce n'est que le début...

# 5 Géants et entreprises du Web

*Sur Internet, il existe bien des services dont beaucoup auraient du mal à se passer, de Google à Facebook en passant par Twitter. Sans même parler de grandes entreprises américaines ou de réseaux sociaux, car de nombreux services sont rendus par de petites entreprises.*

L'utilisation de tels services, grands ou petits, à titre personnel, n'est pas incompatible avec l'anonymat. Il est possible de les utiliser tout en minimisant leurs éventuels effets négatifs sur la vie privée, en maîtrisant ses données personnelles et l'utilisation, parfois complexe, de ces services : nous verrons cela dans la première partie de ce chapitre.

Par ailleurs, il est possible de mener une vie sociale publique sur les réseaux tout en réservant (et préservant !) son anonymat à d'autres activités en ligne. Il ne suffit pas d'éviter de s'inscrire sur les réseaux sociaux : ces derniers sont capables

d'agréger certaines de nos données, même si nous ne visitons pas leurs sites. Nous le verrons dans la seconde partie de ce chapitre.

De nombreux services auxquels nous nous inscrivons ont des politiques discutables vis-à-vis des données personnelles de leurs utilisateurs. Une enquête du site spécialisé Ars Technica a montré qu'environ 20 % d'entre eux se réservaient le droit de revendre vos données personnelles[132].

Bref, pour rester anonyme, il faut faire attention aux endroits où nous choisissons de fournir des données personnelles.

### Filous Collecte de données à l'insu des internautes

Le *Wall Street Journal* rapporte le cas d'une entreprise spécialisée dans la collecte d'informations en ligne sur les clients des concessionnaires des automobiles Dataium. Cette entreprise a placé sur un certain nombre de sites un petit programme, d'apparence totalement inoffensive. Il fallait que plusieurs bouts de programme s'assemblent entre eux pour que le programme final soit complet et que le but de la manœuvre apparaisse clairement : pister les futurs acheteurs d'automobiles.

## Comment savoir quelles traces j'ai laissées ?

Vous avez décidé de reprendre la main sur votre vie en ligne et de regagner un peu d'anonymat ? La première chose à faire est sans doute de constater l'étendue des dégâts. Faites-vous au moins une idée un peu plus précise des informations, éventuellement personnelles, que vous avez laissées aux quatre coins du Web.

## Traces volontaires

Une recherche sur Google sera sans doute des plus utiles. Dans un second temps, vous pouvez essayer le moteur de recherche Pipl.com, qui vous offrira une perspective un peu différente des moteurs traditionnels et révélera peut-être quelques surprises quant à ce que vous avez déjà publié en ligne (dans le cas de l'auteur de ces lignes, l'âge et les études), que ce soit sur des réseaux sociaux, des blogs, des forums ou de simples pages web.

### Astuce La recherche d'images inversée

**L'utilisation de la recherche d'images inversée de Google (accessible depuis google.fr, onglet *Images* puis un clic sur l'appareil photo grisé qui apparaît lorsque l'on passe sa souris sur le champ de recherche) est étonnante : en l'utilisant avec une des photos que vous utilisez fréquemment comme illustration de profil sur Internet, il vous sera peut-être possible de retrouver des informations perdues de vue. Mais si, souvenez-vous, ce compte Myspace créé en 2005 !**

## Traces involontaires

Nous laissons beaucoup de traces involontaires, au gré de notre navigation sur Internet.

Il est possible de voir ce que Google, et plus particulièrement sa régie publicitaire Doubleclick, possède en termes d'informations publicitaires à notre propos, à l'adresse google.com/settings/ads/onweb/. Notez que si vous avez supprimé totalement les cookies de votre navigateur ou si vous avez paramétré ce dernier pour qu'il les efface à chaque fin de session, Google ne devrait rien avoir à se mettre sous la dent.

# Évaluer les risques en souscrivant à un service

Si vous souhaitez utiliser un service proposé par une entreprise sur Internet (réseaux sociaux ou autres), il faut prendre toute la mesure des risques qu'encourt votre vie privée (et votre anonymat).

## Conditions générales d'utilisation, « terms of service » et politiques de vie privée

Vous avez sans doute déjà succombé au mensonge le plus répandu du Web. C'est ainsi que l'on appelle le geste que des milliers d'internautes font chaque jour : cliquer sur *Accepter* au bas des dizaines de paragraphes que constituent généralement les conditions générales d'utilisation (CGU).

Ces textes, qui réglementent l'utilisation des services en ligne, contiennent des dispositions qui encadrent (du moins en théorie) l'utilisation que le site sur lequel vous vous inscrivez peut faire de vos données. Parfois, ces dispositions sont contenues dans les *Terms of service* ou dans les politiques de vie privée (*privacy policies*).

Il suffit de jeter un coup d'œil[133] aux CGU de quelques-uns des principaux sites web (notamment les réseaux sociaux, mais ce constat s'applique à tous les sites) : tous, ou presque, prévoient l'envoi de données identifiantes à des tiers, se réservent le droit d'utiliser votre contenu de la manière qu'il leur plaira, enregistrent les identifiants uniques des appareils que vous utilisez pour vous connecter, collectent des informations via des cookies ou d'autres programmes, retiennent votre adresse IP… Et la liste ne s'arrête pas là. Un récapitulatif de ce que vous avez accepté en vous enregistrant sur Google,

Facebook, Twitter et Instagram a été réalisé par le Tactical Tech Collective (en anglais).

> myshadow.org/lost-in-small-print

### Banalisation Des conditions d'utilisation qui se ressemblent

Une recherche exacte sur la phrase (en anglais) « De cette manière, les serveurs publicitaires pourront compiler des informations sur la manière dont vous ou d'autres utilisateurs de votre ordinateur, ont vu leur publicité » renvoie 460 000 résultats !
Une autre, cette fois portant sur « [le service] révèle des informations identifiantes ou potentiellement identifiantes [à ses] employés, partenaires commerciaux et organisations affiliées » renvoie plus d'un million de réponses !

On ne peut pas faire grand-chose contre ces utilisations et cette collecte de nos données personnelles, à l'exception de refuser d'utiliser ces services.

### Fastidieux Un mois pour tout lire !

Il faudrait un mois de lecture continue à un utilisateur lambda pour lire toutes les CGU des sites qu'il visite pendant une année[134].

Le site Terms of Service; Didn't Read (tos-dr.info) peut être une étape intéressante lorsque vous vous apprêtez à créer un compte sur un service web. Sa petite équipe de juristes a lu les politiques en matière de vie privée de quelques-uns des principaux sites du Web (de Facebook à Google en passant par Wikipédia) et a noté leur pratique en matière de respect des données personnelles de leurs utilisateurs. Ils ont ainsi listé les points positifs, les points négatifs et ont attribué, dans certains cas, une note globale.

Dans le même esprit, une organisation de défense des libertés sur Internet, l'EFF, a réalisé un audit complet des politiques de gestion des données personnelles de quelques-uns des principaux sites web[135]. Dans un tableau synthétique, elle passe en revue quelques grands critères : faut-il un mandat pour que l'entreprise fournisse des données personnelles ? Se bat-elle pour protéger ses utilisateurs devant les tribunaux ? Informe-t-elle l'utilisateur lorsqu'un gouvernement a requis ses données personnelles ? Voilà un bon moyen de voir en un coup d'œil quels services respectent et protègent la vie privée.

### Bouclier La loi de 1978

**La législation française (voir le chapitre 3) est plutôt protectrice en matière de données personnelles, notamment avec la loi de 1978, qui permet de s'opposer au traitement des données personnelles ou de demander leur suppression. Le problème est qu'assez peu de données sont effectivement stockées en France ou exploitées par des entreprises basées dans l'hexagone. Il est difficile de faire jouer cette loi vis-à-vis d'une firme américaine.**

L'extension Privacyfix (Chrome et Firefox) est intéressante : elle montre, sur chaque site que vous visitez (et qui a été inspecté par la communauté), la politique adoptée en matière de données personnelles. Par ailleurs, elle bloque un certain nombre de traceurs et permet, via le site https://privacyfix.org, d'auditer les paramètres de confidentialité que vous utilisez sur les réseaux sociaux.

En ce qui concerne la discrétion sur les réseaux, on évite de nombreux problèmes en prenant simplement du recul sur son utilisation d'Internet et en adoptant de petits réflexes de précaution très simples.

On listera quelques principes de base, applicables à notre sujet, mais également à toute forme de sécurité informatique.

## Les questions à se poser avant d'utiliser un service

Si vous devez vous inscrire sur un quelconque site ou installer un logiciel, voici quelques questions que vous pouvez vous poser pour évaluer le risque encouru :

- Quels types d'informations ce service/logiciel collecte-t-il ? Mon adresse IP, mon adresse e-mail ? Implante-t-il des cookies ?
- Avec qui partage-t-il ces informations ? Des partenaires commerciaux ? Lesquels ?
- Combien de temps garde-t-il ces informations ?
- Est-ce que je peux supprimer les informations que je donne à ce service ou ce logiciel, voire mon compte en entier ?
- Quelles options puis-je modifier dans les paramètres du service ?

Enfin, il faut bien évidemment garder à l'esprit que les géants du Web (ou les moins géants) se conforment aux lois du pays dans lequel ils opèrent, quelles qu'elles soient. Ils peuvent afficher leur attachement à la vie privée avec force promesses, ils subiront toujours au moins trois incitations : la structure d'Internet, qui tend à garder la mémoire de tout, l'incitation économique à gagner de l'argent et monétiser leurs services et enfin une incitation légale, celle qui pousse à obéir à la loi du pays dans lequel ils se situent. Il est toujours difficile de résister à un mandat ou à un policier qui frappe à la porte[136]. Dans bien des cas, la meilleure protection vis-à-vis de ces services pour votre anonymat, c'est l'abstention.

# Protéger son identité chez les géants du Web

Certains disent que, si on ne veut pas que quelque chose soit public, il ne faut pas le publier sur Internet (et ils n'ont pas tout à fait tort). D'autres, comme l'auteur de ce livre, pensent que puisque l'anonymat n'existe pas dans l'absolu, il peut exister en relatif : il est possible d'être anonyme pour son collègue, son patron, tout en utilisant quantité de services en ligne (sans être en rien anonyme vis-à-vis d'eux). Entre les « ayatollahs » de la vie privée et les adeptes du naturisme numérique, existe une troisième voie.

### Prism La collaboration avec les services américains

**Une des plus tonitruantes révélations d'Edward Snowden a été le lien quasi-organique entre certaines des plus grandes entreprises du Web, dont Google et la NSA. Grâce à son programme Prism, cette dernière dispose d'un accès privilégié aux serveurs de ces entreprises, et donc aux données de leurs utilisateurs. Il faut toujours garder à l'esprit cette proximité entre la Silicon Valley et le complexe américain du renseignement. Si vous voulez que vos données échappent à la NSA, leur utilisation est donc à proscrire totalement.**

Il serait un peu court de se borner à l'idée qu'il faut renoncer purement et simplement à Facebook (ou Google) pour préserver sa vie privée.

Le but même d'un réseau social est d'être justement social et publicisé, mais une autre façon de poser la question appelle une réponse moins évidente : peut-on choisir exactement quelles informations on donne à Facebook, notamment afin de protéger son anonymat ou certains aspects de sa vie privée ? Peut-on utiliser les réseaux sociaux en maîtrisant son identité et en restant anonyme par ailleurs ? La réponse est (plutôt) oui.

## Le cas Google

Google a ceci de particulier qu'il offre la gamme de services la plus large du Web : recherche, carte, e-mail, calendrier, documents, actualités… Autant d'éléments qui ont fait son succès et qui ont grandement façonné la manière dont s'est développé Internet. Cette grande variété a pour conséquence que l'entreprise est en mesure de capter une grande partie des activités des internautes et de les conserver dans son écosystème, ce qui pose problème en matière d'anonymat et de vie privée.

### Astuce Moteurs de recherche

**Il est possible d'utiliser des moteurs de recherche sans que ceux-ci en sachent trop sur vous. Plusieurs moteurs se targuent de respecter votre vie privée et de ne pas vous tracer. On citera par exemple IXquick, DuckDuckGo ou StartPage. Il est également possible d'utiliser un moteur de recherche via un proxy web (voir le chapitre 7). Enfin, citons TrackMeNot, une extension amusante développée par l'université de New York. Compatible Firefox et Chrome, elle fonctionne en permanence dans le navigateur et envoie des requêtes aléatoires aux moteurs de recherche afin de noyer les requêtes authentiques de l'utilisateur dans un nuage de fausses demandes.**

Pour commencer, le service Google Dashboard (google.com/dashboard/) est très utile puisqu'il expose tout ce dont les services Google disposent à votre propos. Il propose des accès simples et rapides aux politiques de confidentialité et aux pages permettant de supprimer ses données.

Google propose aussi un service qui vous envoie à intervalles réguliers un rapport sur votre utilisation des services Google (google.com/settings/activity/). C'est un bon moyen de voir à quel point Google peut avoir une vision panoramique de nos vies, parfois intime, en ligne.

### Astuce **Morceler son identité**

**Pour continuer à recourir aux services des grandes entreprises du Web, il peut être bénéfique d'éviter d'utiliser tous les outils qu'ils proposent, pour ne pas tomber dans leur écosystème, leur jardin fermé. Ainsi, si on utilise Gmail, peut-être serait-il sage de ne pas utiliser Google, Google Calendar et Google Drive, afin de limiter le nombre d'informations dont dispose Google à votre sujet.**

De nombreuses méthodes existent pour limiter l'emprise de Google sur vos données. Commencez par vous déconnecter de votre compte Google lorsque vous utilisez la recherche (ou les cartes). Il est également possible de visualiser l'historique des recherches Google, s'il est activé, et de le désactiver, ce qui est fortement recommandé (google.com/history/settings). Il est possible de faire de même pour YouTube (youtube.com/my_search_history). Dans les paramètres de Gmail, on peut également désactiver l'archivage automatique de toutes vos conversations sur la messagerie instantanée (utile si quelqu'un parvient à avoir accès à votre compte).

Enfin, soyez prudents si vous disposez d'un smartphone fonctionnant avec Android, le système d'exploitation développé par Google : par défaut, ce dernier active la géolocalisation et la stocke ! Le résultat est une carte glaçante de tous vos déplacements, visible (seulement par vous) sur google.com/locationhistory. Heureusement, il est facile de la désactiver (https://maps.google.com/locationhistory/b/0/settings).

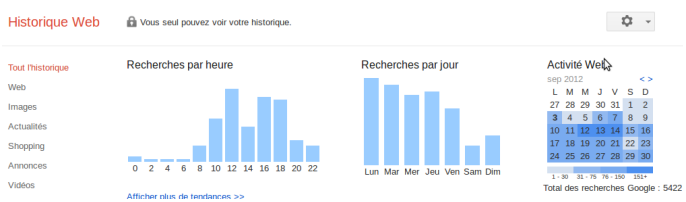



Fig. 5–1 > Extrait d'un historique de recherches Google

### Transparence **Un bon point pour Google**

**Google sait qu'il joue gros sur la question de la vie privée. C'est sans doute ce qui explique la grande clarté et l'exhaustivité de ses pages d'aide concernant cette question. Sur le site google.com/intl/fr/policies/privacy/, vous trouverez un récapitulatif clair et compréhensible des données collectées par Google, le tout en français non juridique. Il propose par ailleurs un guide pour sécuriser vos activités sur ses services.**

> https://www.google.com/safetycenter/everyone/start/

Google dit ne pas utiliser les données du type de celles récoltées par YouTube ou Gmail pour son réseau publicitaire[137], mais l'entreprise utilise cependant des cookies et des traceurs. Si vous désirez que Google cesse de collecter vos données pour afficher des publicités basées sur vos centres d'intérêt, c'est possible à cette adresse google.com/settings/ads/onweb/. On peut également y purger les informations récoltées jusqu'ici. Notez que cette technique consiste simplement à ne plus avoir votre compte Gmail associé directement à votre activité ; cela n'empêche en rien Google de collecter des informations anonymisées, avec toutes les limites que cela peut comporter (voir le chapitre 2).

Les boutons de partage sur les réseaux sociaux, de Google à Facebook en passant par Twitter, sont légions sur les sites web. La présence de ces « bouts de code » un peu partout sur le Web pourrait permettre à ces géants d'Internet de suivre leurs utilisateurs même lorsqu'ils ont quitté le « site amiral ».

### Rassurant **Les géants s'autolimitent**

**Google dit qu'il n'utilise pas les données recueillies par les boutons non cliqués pour son réseau publicitaire, Twitter qu'il ne s'en sert que pour recommander de nouvelles personnes à suivre et Facebook pour des résolutions de bogues[138]. Seule leur parole nous le garantit.**

Plusieurs extensions pour les navigateurs sont disponibles pour contourner la surveillance de Google. L'extension « Do not track me » de l'entreprise Abine (abine.com/donottrackme.html) permet d'effectuer des recherches sur Google sans que ce dernier ne récolte d'informations (compatible avec tous les navigateurs web). Plus anecdotique, l'extension pour Chrome « Google Analytics opt-out », développée par Google, empêche le système de mesure d'audience Google Analytics, présent un peu partout sur Internet, de détecter votre présence.

## Disparaître du Web (et récupérer ses données)

Le meilleur moyen de préserver son anonymat sur Internet est encore de disparaître des réseaux sociaux et des divers services auxquels vous êtes inscrits. Pour un petit service, le plus simple est encore d'adresser un e-mail à l'entreprise qui le fournit afin de procéder à la suppression des données. Si cette dernière est située en Europe, la tâche vous sera facilitée : elle est obligée de supprimer votre compte et ses données associées si vous le lui demandez, en vertu de la législation communautaire. Notez en revanche que certains services basés aux États-Unis ne permettent pas de supprimer son compte !

### Suicide Sortir de tous les réseaux sociaux

La « Suicide machine » (suicidemachine.org) a été développée pour ceux qui voudraient faire le grand saut d'un seul coup. Ce programme vous demande vos identifiants et vos mots de passe ; lorsqu'il se met au travail, il les change tous et supprime vos amis (*followers,* connexions…), rendant votre compte complètement inutilisable et inaccessible. Attention, cette petite astuce ne supprime pas vraiment le compte ; les données restent présentes sur les serveurs et, puisque vous n'avez plus du tout accès à votre compte, il est impossible de les supprimer complètement !

Les principaux services et réseaux sociaux ont mis en place des pages pour supprimer son compte. Elles sont parfois difficiles à trouver :

1. Facebook : facebook.com/help/delete_account. Il est possible également de simplement désactiver son compte : facebook.com/deactivate.php. Attention, Facebook avait défrayé la chronique lorsqu'un étudiant autrichien avait montré que le réseau social ne supprimait pas les contenus même lorsqu'on le lui demandait. La firme de Menlo Park a annoncé qu'elle savait désormais comment faire[139].
2. Google : google.com/accounts/b/0/DeleteAccount.
3. Instagram : instagram.com/accounts/remove/request/.
4. Twitter : twitter.com/settings/accounts/confirm_deactivation.

PAYANT **Faire supprimer ses données**

**De nombreuses entreprises proposent, contre rémunération, de débarrasser Internet des traces que vous avez laissées. L'entreprise Abine propose « Delete Me » (abine.com/marketing/deleteme). Le site Reputation.com est spécialisé dans ce type de nettoyage. Beaucoup d'autres entreprises occupent ce marché. Comme ailleurs, laisser une entreprise gérer le nettoyage de vos données personnelles mérite d'y réfléchir à deux fois.**

## Faire une dernière sauvegarde

Peut-être souhaitez-vous, avant de disparaître de la Toile, télécharger une dernière fois tout ce que vous y avez posté ? Pour ce qui est de vos commentaires de blogs ou autres interventions diverses et variées, la tâche est ardue. Pour les services dits centralisés, c'est plus simple.

Pour Facebook, il existe deux solutions : l'archive simple ou l'archive améliorée. Les deux sont disponibles via un lien figurant sur la page de paramètres (facebook.com/download). Problème : seules 29 % de nos informations personnelles figureraient dans l'archive améliorée fournie par Facebook[140]. En théorie,

selon la loi européenne, il est possible de demander une copie totale de tout ce que Facebook détient. C'est ce qu'a fait un étudiant autrichien, Max Schrems. Depuis, Facebook refuse de répondre à des requêtes similaires, en opposant des délais de traitement trop longs.

Concernant Instagram, on recommandera le site Instaport (instaport.me) qui permet de télécharger toutes ses photos.

Enfin, Google est un des seuls services à proposer un service pour télécharger la quasi-intégralité des données qu'il détient sur vous (google.com/takeout/).

Twitter permet lui aussi de télécharger tous ses tweets, depuis les paramètres.

ALTERNATIVES **Des réseaux sociaux qui respectent votre vie privée ?**

Certains réseaux sociaux annoncent être plus respectueux que d'autres de la vie privée de leurs utilisateurs. Familyleaf ou Path s'en servent comme argument marketing. Au fond pourtant, ces réseaux reposent sur le même modèle économique que les autres et présentent donc les mêmes problématiques. Certains sont plus crédibles, comme Diaspora, un réseau social à but non lucratif, décentralisé et open source. D'autres sont plus expérimentaux (Movim.eu) comme ceux qui fonctionnent en pair-à-pair (Wuala).

## Peut-on faire confiance à un géant du Web ?

Nous avons vu précédemment quelques moyens de préserver sa vie privée face aux géants du Web ou plus simplement de gérer les données qu'on y laisse. Dans une perspective d'anonymat, l'utilisation de ces géants, réseaux sociaux ou non, n'a pas vraiment de sens.

Les réseaux sociaux, même ceux qui assurent être prudents avec vos données, fourvoient leurs utilisateurs dans un faux sentiment

de sécurité[141]. Quelle que soit la nature des « Paramètres de confidentialité » ou autres « Options de vie privée », à partir du moment où une donnée figure sur Internet, elle peut être copiée, redistribuée, automatiquement ou pas : c'est la nature même du réseau ! De plus, ces plates-formes sont soumises à une logique économique. Pour monétiser les données personnelles de leurs utilisateurs, elles cherchent à faire reculer graduellement la limite de la vie privée sur leurs services. Facebook a par exemple une politique dite d'*opt-out* : il impose aux utilisateurs les changements de paramètres, à eux ensuite d'éventuellement les désactiver.

Des chercheurs ont montré que, structurellement, l'utilisateur est incité à se dévoiler sur les réseaux sociaux[142] : les données personnelles sont un « input nécessaire[143] » à ces réseaux. Il est donc illusoire de prétendre avoir une véritable vie privée (ou une intimité) sur un réseau social.

« La perte de contrôle est consubstantielle au comportement d'exposition de soi dans le Web relationnel. S'exposer et prétendre contrôler les effets de cette exposition sont en partie antinomiques car les bénéfices de l'exposition impliquent une certaine perte de contrôle », écrivent Alain Rallet et Fabrice Rochelandet[144]. Cette perte de contrôle est presque insidieuse, écrivent pour leur part Fanny Georges, Antoine Seilles et Jean Sallantin : « L'utilisateur est moins identifié par les données qu'il délivre que par le traçage de ses activités. Toute utilisation du service est productrice d'identité[145]. »

Cela ne doit pas vous empêcher, utilisateurs, de tenir pour responsables les services auxquels vous (ou les internautes de manière générale) faites confiance : connaître les limites de ces réseaux en matière de vie privée ne doit pas être un blanc-seing pour ces derniers. Selon la chercheuse Danah Boyd, être public a des coûts importants. Et lorsqu'une entreprise force ses utilisateurs à être « un peu plus publics », ce sont les plus désavantagés socialement et économiquement qui sont les plus touchés[146].

Traduction **La colère de la chercheuse Danah Boyd**

« Forcer les gens à être publics ne met pas fin aux structures de privilèges et de pouvoir. Ce qui m'ennuie, c'est que ça les renforce. Les privilégiés sont plus privilégiés et gagnent à être exposés. Et ceux qui luttent dans leur vie de tous les jours sont constamment en train de reconstruire les murs qu'on a abattus. Le professeur, la femme battue, l'enfant pauvre qui vit dans le ghetto et qui voudrait en sortir. Comment les prend-on en considération quand on construit des systèmes qui exposent les gens ? […] On ne peut pas se cacher derrière la rhétorique selon laquelle tout est public parce que dans nos cercles privilégiés tout le monde s'en sort avec facilité dans la sphère publique[147]. »

# Déjouer le pistage à notre insu

On a vu dans la première partie de ce chapitre comment mieux maîtriser son identité là où on choisit volontairement de se rendre. Malheureusement, une partie conséquente des intrusions et de la compromission de l'anonymat sur Internet se fait sans même que l'on s'en rende compte.

## Empêcher les réseaux sociaux de nous suivre

Hors de Twitter ou Facebook, vous pensiez être à l'abri ? Loin de là, puisque le nombre de sites qui intègrent les boutons de partage de ces réseaux est en constante augmentation. Et lorsque vous visitez l'un d'eux sans vous être déconnecté de votre réseau social, vous pouvez faire savoir à ce dernier que vous êtes en train de consulter ledit site !

Tenace **Facebook nous suit vraiment partout !**

Un développeur a réalisé que même en se déconnectant de Facebook, celui-ci continue à surveiller la manière dont nous naviguons sur les sites qui comportent le bouton *Like*[148] !

Une première précaution peut être prise en se déconnectant systématiquement des réseaux sociaux une fois votre utilisation terminée. Plus efficace encore : on peut par exemple utiliser des navigateurs différents pour le surf personnel et pour les réseaux sociaux.

### Précision Que fait Twitter de ces données ?

Twitter dit n'utiliser les visites enregistrées de ses utilisateurs sur des sites tiers que pour leur suggérer des comptes à suivre. Il est possible de désactiver cette option dans les paramètres.

L'extension pour Firefox (et Chrome) Share Me Not (sharemenot.cs.washington.edu), développée par une équipe de l'université de Washington, est destinée à empêcher les réseaux sociaux de suivre votre navigation sur les sites qui intègrent leurs boutons de partage. L'université de Berkeley a également développé une extension similaire (priv3.icsi.berkeley.edu), Priv3 (uniquement disponible sur Firefox), qui vous protégera contre les yeux indiscrets de Facebook, Twitter, Google+ et LinkedIn. Pour cette catégorie d'outils, les options ne manquent pas : l'entreprise Disconnect a également développé son extension pour Firefox (disconnect.me). Il est par exemple également possible d'installer les extensions « à la carte » pour se protéger exclusivement de Facebook ou de Twitter.

### Bonus Des recherches non personnalisées

Google a de plus en plus recours à la personnalisation des recherches pour ses utilisateurs. Utiliser ce type d'extension permet justement de se cacher et d'obtenir des recherches non altérées (ou non améliorées, selon le point de vue) et sortir de ce qu'on appelle la « bulle » de recherche, qui a pour conséquence de nous délivrer des résultats proches de nos opinions, comme une sorte de filtre.

## Empêcher les publicitaires de nous suivre

Comme nous l'avons vu dans le chapitre 2, de nombreux acteurs surveillent, en silence, notre activité sur Internet. Heureusement, de nombreux outils très complets existent pour leur faire barrage.

La solution la plus simple et la plus directe consiste à installer un bloqueur de publicité, comme Adblock Plus, le plus connu (disponible pour Chrome, Firefox et Safari). Cette extension se base sur une liste mise à jour par des bénévoles. Pour que son usage soit activé, il faut se rendre dans les paramètres de l'extension et choisir une liste. C'est cette liste qu'il utilisera pour filtrer les publicités (on recommandera l'utilisation de la liste Easylist). Évitez de vous inscrire à plusieurs listes en même temps, elles peuvent interférer entre elles.

L'avantage de bloquer la publicité est double : en plus d'éviter de laisser encore plus de traces, cela peut améliorer la vitesse et le confort de navigation.

PRÉCISION **Outils multifonctions**

**Les outils que nous présentons dans ce chapitre ont beaucoup de points communs. Ainsi, toutes les extensions anti-traçage (Ghostery, Collusion, DNT+) bloquent également les réseaux sociaux. Les installer tous n'est pas forcément une bonne idée : il vaut mieux cibler vos besoins, évaluer la menace et installer les extensions correspondantes.**

Les entreprises qui disposent de traceurs sur Internet font pour la plupart (mais pas toutes) partie d'organisations rassemblant des acteurs de l'industrie publicitaire. Ces dernières ont mis en place un site, aboutads.info, où il est possible en quelques clics de signifier votre désaccord (*opt-out*) avec le fait d'être « tracé » partout sur Internet et de voir des entreprises personnaliser des publicités en fonction de vos habitudes de consommation. Le tout en un clic. Par ailleurs, l'une

des organisations participantes dispose elle aussi de son outil dit d'opt-out, networkadvertising.org/choices. Notez que si vous utilisez les conseils et les outils de ce chapitre, ces entreprises ne devraient de toute façon pas voir grand-chose de ce que vous faites sur Internet.

La fondation Mozilla, qui édite le navigateur Firefox, a quant à elle développé une technologie très intéressante, appelée Collusion. Sous forme d'une extension classique (mozilla.org/en-US/collusion), elle montre tous les sites qui se trouvent sur le chemin de l'internaute, qu'il s'agisse des sites qu'il visite volontairement ou des petits bouts de codes appartenant à des tiers qui s'y trouvent. Il ouvre une fenêtre où apparaissent, au fur et à mesure de la navigation, les sites qui ont été avertis de la présence de l'internaute.

### Astuce Gérer plusieurs identités en même temps

Avoir plusieurs « identités » sur le Web, notamment lorsqu'il faut remplir des formulaires, peut être un moyen efficace de contourner la surveillance. Il est possible de le faire à la main, mais des outils existent pour renforcer la protection.

Abine (encore eux) met à disposition MaskMe, une extension (uniquement pour Google Chrome ; les utilisateurs de Firefox doivent installer une extension qui remplit également d'autres fonctions sur abine.com/apps.php) qui crée à chaque formulaire une adresse e-mail aléatoire : les courriels qui y sont adressés sont ensuite redirigés vers votre boîte e-mail classique, comme une sorte de tampon entre vous et l'entreprise ou le service (notez qu'Abine est aussi une entreprise, il faut donc parvenir à leur faire confiance). L'extension prend également en charge les numéros de téléphone ainsi que les mots de passe.

Si vous voulez vous inscrire à un site ou à un service mais sans lui fournir toutes vos informations personnelles, le site fakenamegenerator.com crée, lui, une identité virtuelle complète (nom, adresse, lieu de naissance…) pour accélérer encore la démarche.

Le site Disconnect (voir plus haut) propose également une extension appelée Collusion, pour Chrome et Safari, qui a un mode d'affichage un peu plus fin et détaillé.

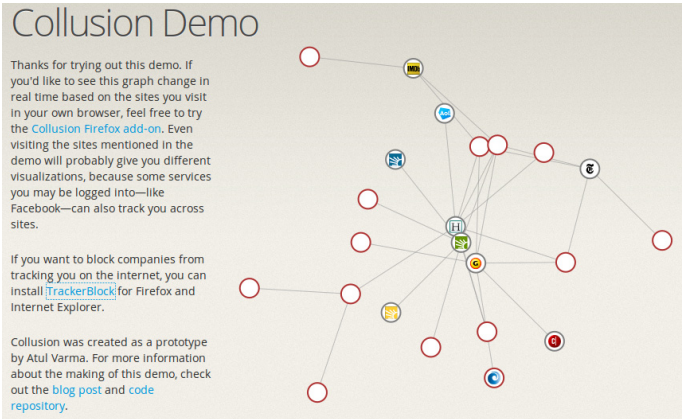



**Fig. 5–2 > Exemple de fonctionnement de Collusion, où chaque bulle représente un site. Cet outil permet de repérer quels sites tiers sont présents sur le site que vous visitez.**

Ce n'est pas forcément une mauvaise chose que de se faire suivre sur Internet par tout un tas d'acteurs tiers : l'apparition de certains sites dans Collusion est logique, notamment parce qu'ils servent à faire apparaître des systèmes de commentaires ou comptabiliser le nombre d'internautes. Il est cependant intéressant de savoir qui exactement est averti de notre passage sur une page.

### Innovation « Do Not Track », please !

Le département du commerce américain a, en mars 2012, appelé les principaux acteurs du secteur à implémenter une fonctionnalité appelée *Do Not Track*[149] (ne pas tracer) : cette innovation consisterait à mettre en place un réglage dans les navigateurs des internautes pour signaler sur leur passage qu'ils ne souhaitent pas être tracés durant leur navigation. Plusieurs acteurs ont déjà agi : Firefox inclut cette option (une simple case à cocher dans les paramètres *Options > Vie privée*) et Twitter a annoncé respecter cette mesure[150]. Il ne s'agit pour le moment que de déclaratif.

Abine a développé une extension pour Chrome, Firefox, Safari et Internet Explorer appelée DoNotTrackMe (abine.com/dntdetail.php). Très simple à prendre en main, elle bloque à la fois les réseaux sociaux et les traceurs. Elle montre aussi le nombre de tentatives d'intrusion empêchées depuis le début de son utilisation.

Entreprise surfant sur la demande des internautes en matière de vie privée, Abine a plusieurs projets dans ses cartons (abine.com), dont certains visent à protéger votre numéro de téléphone ou à simplifier et sécuriser l'identification sur des sites requérant un mot de passe. Ils sont pour le moment disponibles en version d'essai.

### Chiffres L'anti-tracking séduit

**Près de 17 millions d'internautes utilisent Adblock plus. La firme Abine estime quant à elle que près de 28 millions d'utilisateurs ont recours à une technologie anti-tracking, soit une augmentation de 50 % en un an[151].**

Une star des plug-ins anti-tracking s'appelle Ghostery. Elle est similaire à DoNotTrackMe, à la différence que la liste des traceurs et autres espions qu'elle bloque est définie par 300 000 de ses utilisateurs[152]. Sur le site de Ghostery, chacune des 1 200 entreprises que l'extension se vante de bloquer dispose d'une fiche détaillant ses pratiques en matière de vie privée et de négoce des données de navigation qu'elles récoltent. Notons enfin que comme DoNotTrackPlus, Ghostery est développé par une entreprise privée, Evidon.

Un dernier a fait récemment son apparition sur ce secteur : PrivacyBadger (https://www.eff.org/privacybadger). Développé par une très fiable organisation de défense des libertés sur Internet, l'Electronic Frontier Foundation, elle remplit la plupart des fonctionnalités des outils précédemment évoqués. En

revanche, à l'inverse des autres, elle n'est pas l'œuvre d'une entreprise, ce qui en fait une solution à privilégier.

Pour les utilisateurs les plus avancés, l'utilisation de l'extension (Firefox) NoScript peut être recommandée. Elle bloque les morceaux de codes JavaScript qui peuvent être utilisés pour récolter des informations concernant l'internaute. Le principal problème, c'est que le Web d'aujourd'hui utilise massivement JavaScript, dans la majorité des cas pour des buts très louables (rendre une page plus agréable, la doter de nouvelles fonctionnalités). Il est possible de paramétrer cette extension pour qu'elle accepte le JavaScript sur certains sites de confiance que l'utilisateur peut définir lui-même. Il existe une adaptation de cette extension pour Chrome, ScriptNo.

Pour ces mêmes utilisateurs, on pourra mentionner l'extension pour Firefox Better Privacy qui bloque les LSO, ces cookies Flash cachés assez profondément dans le navigateur.

D'autres extensions au fonctionnement similaires existent comme TrackerBlock, TACO ou AdHacker.

## Quelques principes avant de télécharger une extension ou un programme

Nombreux sont les outils évoqués ici qui sont développés et édités par des sociétés privées. Peut-on vraiment leur faire confiance ?

Cela dépendra de vous et de la confiance que vous placez en ces services (et ceci est valable de manière générale avec toutes les entreprises que vous croisez sur Internet).

Quelques principes doivent guider votre choix :

- Ai-je la maîtrise et/ou la propriété de mes données personnelles ?
- Suis-je mis au courant de la façon dont mes données sont stockées, exploitées, éventuellement transmises à des tiers ?

- Les données que je fournis sont-elles rigoureusement nécessaires à la fourniture du service que je demande ?
- La transmission de données à des tiers est-elle nécessaire pour le service rendu ? Mes données sont-elles revendues ?

Il faut garder à l'esprit en toutes circonstances qu'il vaut mieux faire confiance à du code ouvert qu'à une entreprise. Même si on peut penser que les services qu'on nous rend en échange de nos informations personnelles sont intéressants, les entreprises auront toujours leurs propres priorités. Comme le dit Marcus Ranum, développeur et expert en sécurité informatique[153] : « Moi ? Je ne m'inquiéterai de Big Brother que lorsque le gouvernement fédéral commencera à embaucher les gars qui ont fait Amazon.com, Google, eBay et Yahoo!. »

# 6 Communiquer : e-mails et discussions instantanées

*L'e-mail est un outil de communication incontournable, mais qui peut être très dangereux pour votre anonymat.*

## Qu'est-ce qu'un e-mail ? Comment circule-t-il ?

Avant d'apprendre à se protéger, il faut d'abord comprendre ce qui se passe lorsque l'on consulte ou envoie ses e-mails.

## Un peu de vocabulaire

**Serveur de mail.** C'est l'ordinateur (un serveur) qui gère l'envoi, la réception et le stockage de vos e-mails. Attention, ce n'est pas le logiciel que vous utilisez pour envoyer vos e-mails : imaginez plutôt le serveur comme un site auquel vous êtes le seul (en théorie) à avoir accès, sur lequel vous attendent vos e-mails et depuis lequel vous pouvez en envoyer.

**Messagerie** ou **client e-mail.** C'est le logiciel qui vous permet de consulter vos e-mails (qui va interroger votre serveur pour vérifier la présence de nouveaux messages) ou d'en envoyer (qui va charger le serveur d'envoyer un message électronique). Les plus connus sont Thunderbird (que nous recommandons, c'est l'équivalent de Firefox) ou Outlook.

**Webmail.** C'est l'équivalent d'un client e-mail depuis un site Internet. Les plus connus sont Gmail, Outlook.com ou Yahoo! (même s'ils sont également accessibles depuis un client mail).

## Différence entre les protocoles de courriel POP et IMAP

POP (port 110), parfois appelé POP3, est un protocole qui permet de télécharger les e-mails depuis votre compte jusqu'à votre client. Une fois récupérés, les e-mails sont détruits du serveur. Certains clients proposent d'en conserver une copie sur le serveur.

IMAP (port 143) est un protocole qui manipule les e-mails contenus sur le serveur sans les télécharger sur l'ordinateur. Toutes les opérations sont effectuées sur le serveur, les e-mails ne le quittent jamais. Cette utilisation est recommandée si vous travaillez sur plusieurs ordinateurs.

**Sûreté Encore plus confidentiel**

**Une version sécurisée des protocoles POP et IMAP passe respectivement par les ports 995 et 993 (si vous utilisez un client e-mail, il est facile d'aller vérifier cela dans les paramètres).**

## Les vulnérabilités de l'e-mail

Lorsque vous envoyez un courriel, votre client e-mail ou votre webmail fait parvenir des instructions à un serveur d'e-mail. Ce dernier, si vous décidez d'envoyer un message, va se comporter comme votre navigateur pour un site web : il va « se promener » de serveur en serveur, copiant et recopiant votre message pour le faire parvenir au serveur mail de votre destinataire. Et, comme la navigation est souvent non protégée, son contenu est très facilement accessible. En réalité, dans la plupart des cas, un e-mail n'est pas plus privé qu'une carte postale.

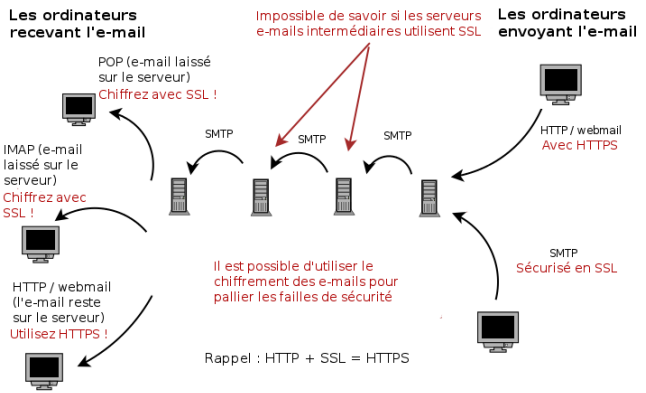



Fig. 6–1 > Schéma du trajet typique d'un e-mail (adapté de ssd.eff.org)

Google a récemment publié un rapport très éclairant[154]. Grâce à la position de force de son service d'e-mail, Gmail, il est en première ligne pour voir si les autres fournisseurs, avec qui les utilisateurs de Gmail correspondent, chiffrent les e-mails lors de leur acheminement. Le résultat est en amélioration constante, mais encore insuffisant : 70 % des courriels envoyés depuis Gmail sont chiffrés pendant tout leur transit, moins de 50 % pour les messages parvenant à Gmail.

Le géant de la recherche se permet même de nommer les mauvais élèves : en France, lorsqu'on envoie depuis Gmail un message à destination d'une adresse en orange.fr ou free.fr, il n'est quasiment jamais protégé. Cela s'explique par le fait que pour qu'un e-mail soit chiffré pendant tout son cheminement, il faut que les deux fournisseurs mettent en place cette protection.

COMPARAISON **Aux États-Unis, le téléphone mieux protégé que l'e-mail**

Il est bien plus facile pour les autorités américaines de surveiller quelqu'un via ses e-mails que via son téléphone[155]. En effet, pour les courriels vieux de plus de six mois et ceux qui ont été lus, la police n'a pas besoin d'un mandat. La législation qui peut vous protéger des interceptions de communications ne s'applique pas aux courriels.

Outre une interception ou une copie à n'importe lequel des points de son trajet, il est possible de voir dans l'en-tête d'un courriel tout ce qui vient avant le début du message, ce qui donne des informations importantes, comme par quel serveur il a transité et parfois même l'adresse IP d'envoi !

EN PRATIQUE **Voir l'en-tête avec Gmail**

Depuis Gmail, vous pouvez visualiser l'en-tête d'un courriel en cliquant sur la petite flèche en haut à droite de chaque message puis sur *Voir source* ou *Afficher l'original*.

On a longtemps dit qu'un bon moyen pour échanger des e-mails de manière confidentielle était de le faire sur le dossier brouillon. Le premier interlocuteur crée un nouveau message, le rédige mais ne l'envoie pas et le stocke en brouillon. Le second interlocuteur n'a plus qu'à se connecter et récupérer le message. Cela suppose que les autorités tentent d'intercepter l'e-mail lorsqu'il est émis, alors qu'en réalité, lorsqu'elles mènent l'enquête, elles demandent l'intégralité du compte, brouillons compris[156]. De plus, dans la plupart des cas, le brouillon doit être stocké, donc envoyé sur un serveur distant à des fins de sauvegarde, comme un e-mail classique. La technique du brouillon peut être intéressante si les deux interlocuteurs prennent de grandes précautions pour y accéder (Tor, VPN, ou d'autres solutions que nous aborderons dans le chapitre 7).

De plus – cette évidence mérite d'être rappelée –, lorsque vous envoyez un e-mail, ce dernier sort de votre contrôle. Il pourra être copié, distribué, stocké ou non, sans que vous en soyez informé. Supprimer un e-mail ne le supprime que sur votre propre serveur, pas sur celui de vos correspondants.

En termes de protection, l'échange d'e-mails recouvre trois dimensions :

- la confidentialité (seul le destinataire du message le lit) ;
- l'authenticité (on est sûr que la personne qui le reçoit est la bonne) ;
- l'intégrité (on est sûr que le message n'a pas été altéré).

Un échange d'e-mails peut laisser passer plusieurs types d'informations : l'identité des deux personnes qui échangent, le contenu de leurs messages, les services qu'ils utilisent, la date et l'heure, parfois le lieu d'envoi de l'e-mail… Les outils et les réflexes que nous allons aborder ne protègent pas toutes les dimensions simultanément : il faudra donc savoir et comprendre comment les manipuler.

# Comment choisir votre fournisseur de mail ?

Il ne faut pas utiliser le serveur d'e-mail de votre fournisseur d'accès à Internet (orange.fr, free.fr, etc.). Ce dernier peut déjà savoir comment vous naviguez, ce n'est pas la peine de lui donner encore plus d'informations ! À choisir, l'utilisation de comptes comme Gmail ou Yahoo! est donc préférable.

## Les webmails commerciaux

Les webmails commerciaux sont pratiques puisqu'ils permettent d'accéder à ses messages passés et présents depuis n'importe quel terminal, fixe ou mobile. Cependant, ce n'est pas une solution des plus efficaces en termes d'anonymat et de protection de la vie privée, puisque vous ne pouvez pas télécharger vos messages, et n'accédez toujours qu'à une copie de ces derniers. Cela manque de protection, notamment si votre adversaire dispose de moyens légaux : il est beaucoup plus facile d'obtenir, via un mandat, l'accès à une boîte mail contenant toutes les communications plutôt que de les intercepter une à une à leur envoi. C'est d'ailleurs la solution la plus fréquemment utilisée par les forces de l'ordre ; la NSA, par exemple, dispose, comme on l'a vu précédemment, d'un accès privilégié à un certain nombre de fournisseurs de courriels, comme Yahoo! ou Google.

Il est cependant possible de s'enregistrer auprès d'un webmail, puis d'utiliser son adresse et de relever son courrier depuis un client, et de paramétrer ce dernier pour qu'il supprime du serveur les messages dès qu'il les a consultés. Les principaux webmails proposent cette option (dont Yahoo! et Gmail).

Il faut également avoir en tête que des entreprises comme Google ou Yahoo! collaborent régulièrement avec les autorités et la justice. Elles n'hésitent pas à leur fournir des données

concernant leurs utilisateurs. Par ailleurs, lorsque vous supprimez un message de leur serveur, il est très probable que des copies subsistent sur d'autres machines. Enfin, Google scanne le contenu de vos e-mails pour vous proposer de la publicité ciblée.

Cependant, un webmail commercial peut être assez fortement anonyme, notamment si vous utilisez un pseudonyme et si vous créez votre compte avec une protection suffisante (comme Tor, voir le chapitre 7). Il faudra utiliser ce logiciel pour vous connecter à cette boîte systématiquement. La seule vulnérabilité, c'est la propension de ces entreprises à répondre aux demandes légales et le fait qu'il n'est jamais tout à fait certain que vos messages soient supprimés.

### Choix Faut-il choisir Gmail ?

**Choisir Gmail ou d'autres solutions issues de géants américains dépend beaucoup de la confiance que vous mettez dans Google (elle devrait être plutôt faible), mais également de la menace contre laquelle vous devez vous protéger (un état autre que les États-Unis pourra avoir du mal à accéder à votre boîte Gmail). Il faut également prendre en compte la probabilité accrue de passer inaperçu avec une banale adresse Gmail.**

## Solutions d'e-mail alternatives

Une solution radicale consiste à mettre en place son propre serveur de mail (dans son salon par exemple). Si cela ne protège pas du tout contre une saisine par les autorités de votre pays, c'est en revanche une très bonne protection vis-à-vis des géants du Web, puisque vous avez un contrôle parfait sur ce qui est stocké et conservé. Ce problème peut être contourné si vous chiffrez systématiquement vos e-mails (mais il faudra paramétrer votre client e-mail de manière assez fine pour utiliser un VPN ou Tor).

Des services et des organisations fournissent cependant des comptes e-mails réputés sûrs, dont l'intérêt réside surtout

dans leur résistance aux autorités (notamment parce qu'elles sont situées dans des législations protectrices).

Riseup (riseup.net) est une organisation réputée pour fournir des solutions fiables et sécurisées à un grand nombre d'activistes dans le monde entier. Ils appliquent une politique de confidentialité très stricte. L'avantage, c'est que ce n'est pas une entreprise et qu'ils ne poursuivent donc pas d'intérêt commercial : il faut d'ailleurs être invité par un membre déjà inscrit pour pouvoir créer un compte.

### Loi Cela ne les place pas hors de portée des autorités

**En avril 2012, le FBI, dans le cadre d'une enquête sur des menaces à la bombe à l'université de Pittsburgh, a saisi[157] un serveur informatique appartenant au Riseup network et à May First/People Link. Le problème ici n'est pas vraiment la compromission de l'anonymat : selon ses responsables, le serveur n'aurait contenu aucune information puisqu'il était conçu pour ne conserver aucun registre des connexions de ses utilisateurs[158] et ne permettrait donc aucune identification. Cette saisie aurait tout de même interrompu le service pour de nombreux utilisateurs.**

Hushmail, une entreprise basée au Canada, propose également un service d'e-mail très compétitif, également réputé pour être sécurisé : il a été utilisé par un agent de la très secrète NSA qui voulait dénoncer les exactions de ses supérieurs[159]. Cela ne l'empêche pas, dans certains cas, de fournir des données concernant ses utilisateurs quand la police les lui demande[160].

Il est également possible de chiffrer ses e-mails directement depuis le webmail d'Hushmail, soit grâce un petit logiciel que vous devez installer, soit directement sur leur serveur (cette solution est moins sûre). Des soupçons existent cependant quant à leur capacité à déchiffrer ces e-mails à la demande des autorités.

Le service est gratuit mais limité : pour obtenir davantage d'espace de stockage, il faut sortir le porte-monnaie (et donc laisser éventuellement une trace très identifiable). Notons également que si communiquer avec un interlocuteur utilisant égale-

ment Hushmail peut être sûr, toute sécurité est fortement altérée si vous communiquez avec une adresse Gmail ou Yahoo!.

Profitant du début de prise de conscience mondiale engendrée par les révélations d'Edward Snowden, de nombreuses entreprises ont mis la protection de la vie privée et le chiffrement au cœur de leur stratégie et de nouveaux acteurs sont arrivés sur ce marché. On pourra citer par exemple Lavaboom.com, Virtru.com et Protonmail.ch, entre autres. Il y a plusieurs choses à avoir en tête concernant ces trois services. D'abord, il s'agit souvent de versions bêta, en cours de développement : de nouvelles fonctionnalités plus poussées sont généralement prévues. Cela peut aussi vouloir dire que des failles de sécurité peuvent être présentes dans leur code ou leur infrastructure. Par exemple, certains d'entre eux utilisent une interface web, dont la sécurité, concernant le chiffrement, est loin d'avoir fait ses preuves. Par ailleurs, ils ne sont pour la plupart pas basés aux États-Unis, ce qui est une bonne chose. Ces solutions peuvent être intéressantes, même si on manque, au moment d'écrire ces lignes, de recul concernant leur réel niveau de sécurité.

### Liens D'autres services d'e-mail

Il existe de nombreux services et organisations intéressants proposant des services d'e-mail :

> sud-ouest.org
> mailoo.org
> legtux.org
> safe-mail.net
> s-mail.com
> neomailbox.com
> mutemail.com
> vmail.me
> inventati.org
> toonux.net
> anonbox.net
> PRQ.se

Pour savoir si un fournisseur d'e-mail est digne de confiance, voici quelques questions à se poser :

- Que dit sa politique de vie privée ? Est-elle protectrice vis-à-vis de vos données ?
- Vous avertit-il si les autorités veulent accéder à vos conversations ?
- Dans quel pays seront hébergées vos données ? Préférez le Canada, l'Allemagne, la Suisse, l'Islande ou la Suède aux États-Unis.
- Conserve-t-il des traces de vos conversations ? De vos connexions à votre compte ?

Attention, l'utilisation de comptes connus pour leur sympathie envers les dissidents de toutes sortes (comme Riseup) présente le risque d'être plus facilement repérable, à l'inverse d'un compte classique comme Gmail. Si vous contactez quelqu'un sous surveillance, cela attirera l'attention.

## Se protéger

La plupart du temps, lorsque vous consultez vos e-mails, via un webmail mais aussi et souvent via un client (configuré en IMAP), vous ne faites qu'accéder à une copie du message reçu, qui reste stocké sur les serveurs de votre fournisseur d'e-mail, ce qui pose quelques problèmes en termes de vie privée. Si vous utilisez un client, il faut donc le configurer pour qu'il supprime les messages dès qu'il y a accédé (POP, généralement depuis les paramètres).

Évidemment, vous perdez en rapidité et en pratique ce que vous gagnerez en sécurité, puisque vous ne pourrez accéder à vos e-mails que depuis une seule machine. De plus, il faut garder à l'esprit que dans le cas des gros fournisseurs d'e-mail, même lorsque vous appuyez sur le bouton *Supprimer*, une copie est susceptible d'être conservée pendant une durée

indéfinie sur les serveurs (notamment parce qu'il existe des copies de sauvegarde sur plusieurs machines). Une solution peut être de chiffrer vos e-mails (voir plus loin) : dans ce cas, même avec une copie de vos messages, votre fournisseur d'accès à Internet ou votre fournisseur de mail ne pourra rien en faire.

Il peut être très utile de ne donner son véritable nom sur les réseaux qu'en tout dernier recours pour protéger votre identité vis-à-vis des entreprises qui peuplent le Web. Cela peut être fait par la création de nombreuses fausses adresses (voir page suivante), ou tout simplement en compartimentant. On peut ainsi imaginer ne donner aux entreprises et services variés qu'une adresse e-mail à pseudonyme, qui ne contient pas votre nom civil. Par ailleurs, on peut utiliser deux adresses e-mails (les deux pseudonymes), l'un pour la vie « publique » (réseaux sociaux, achats en ligne, correspondance professionnelle) et une autre pour l'activité personnelle (rencontre, discussions…).

### Attention Les ordinateurs d'entreprise

**Lorsque vous utilisez votre ordinateur professionnel, rien n'empêche l'administrateur du réseau de surveiller ce que vous faites avec votre connexion. En réalité, seuls les e-mails comportant la mention « personnel » dans leur sujet ne peuvent pas être ouverts par votre entreprise (et encore ! La justice y met une exception en cas de risque ou d'événement exceptionnel). Et si le règlement intérieur de votre entreprise ne le précise pas, vos e-mails professionnels peuvent être ouverts en votre absence[161].**

Plus technique, il faut s'assurer que vous consultez votre webmail à l'aide d'une connexion sécurisée, en HTTPS (voir le chapitre 4). Elle est en théorie activée par défaut sur Gmail, Hotmail, Yahoo! et Outlook. Sans cette connexion sécurisée, tout ce que vous faites sur votre boîte e-mail peut être facilement intercepté. Attention, certains webmails utilisent le

HTTPS pour la connexion, mais pas pour la consultation ou l'envoi des messages. Pensez à vérifier la présence du cadenas ou de la coloration dans votre barre d'adresse.

**Astuce Comment créer un compte e-mail totalement anonyme ?**

Il faut d'abord créer un compte, par exemple sur Hushmail, en utilisant Tor (voir le chapitre 7). Si vous ne le faites pas, votre adresse IP sera associée à la création du compte. Ensuite, il faudra toujours et systématiquement se connecter à votre boîte aux lettres en utilisant Tor et une connexion en HTTPS : un seul oubli et votre adresse IP sera associée à une consultation du compte et/ou à un envoi de message ! Hushmail est un des seuls fournisseurs d'e-mail à permettre l'utilisation de Tor sur ses services. Il est possible de recourir à une solution moins sécurisée mais plus souple, celle du VPN, pour consulter et envoyer ses messages (voir le chapitre 7). Si, en plus de ces précautions, vous apprenez à chiffrer efficacement vos e-mails, votre niveau de protection sera assez élevé[162]. Si vous utilisez un client e-mail, il est généralement possible de le paramétrer pour qu'il utilise un proxy ou un VPN.

## Adresse e-mail jetable : vers un e-mail propre

En théorie, pour échapper au profilage des entreprises sur le Web, il faudrait utiliser une adresse e-mail par service, entreprise ou site sur lequel on est inscrit – voilà qui est compliqué ! Ici, nous ne parlons pas vraiment de solution pour l'anonymat, mais d'un moyen de compartimenter les informations auxquelles ont éventuellement accès les entreprises sur Internet (ce qui est un moyen très puissant de protéger sa vie privée). Les services permettant ce type de protection sont nombreux.

Spamgourmet.com est la solution la plus évoluée. Après avoir créé votre compte sur le site (et fourni votre véritable adresse e-mail), vous pourrez créer à la volée des adresses e-mail dès que

l'on vous en demandera une, sans même avoir à retourner sur le site. Vous pouvez dans le même temps spécifier le nombre maximal d'e-mails que cette adresse pourra recevoir. Ensuite, tous ces messages sont transférés sur votre véritable adresse. Si une entreprise commence à vous solliciter un peu trop souvent, il suffit de supprimer l'adresse intermédiaire. Et cela permet surtout d'éviter de donner sa véritable adresse aux entreprises (et d'en donner une différente par entreprise ou service).

Yopmail.com a un fonctionnement un peu différent, mais plus simple. Le site propose de vraies boîtes e-mail, qui peuvent être créées sans même se rendre sur le site. En fait, toutes les adresses existent déjà, il suffit par exemple de se rendre sur yopmail.com?livreanonymat et la boîte de réception de livreanonymat@yopmail.com apparaît, ainsi que les messages qui y ont été adressés. C'est à la fois très utile pour la confidentialité vis-à-vis des entreprises à qui vous allez donner une vraie/fausse adresse Yopmail, puisque cette dernière n'est absolument pas liée à votre adresse originelle. En revanche, n'importe qui disposant de votre adresse peut voir les messages qui y arrivent ; ce n'est donc évidemment pas destiné à un autre but que celui d'éviter le spam et de compartimenter votre vie en ligne.

Pour contourner un peu ce problème, Yopmail fournit pour chaque adresse un alias (visible au dessus de la boîte de réception). Ce dernier peut être diffusé partout : il ne donne pas accès à la boîte e-mail et transfère les messages qu'il reçoit vers la boîte e-mail. Il est possible d'envoyer des e-mails, mais uniquement vers une autre adresse Yopmail. Il y a également une extension pour Firefox (yopmail.com/plugins.php).

Nous recommandons également 10minutemail.com (comme son nom l'indique, la boîte mail n'est accessible que pendant 10 minutes), mail-jetable.appspot.com (durée de validité configurable), jetable.org/fr/index (qui dispose aussi d'une extension Firefox), tempomail.fr (permet de créer un alias permanent qui redirige vers votre vraie boîte mail et dispose d'une extension Firefox), getonemail.com,

mailinator.com (similaire à Yopmail), meltmail.com (service de redirection temporaire), trashmail.net (avec une extension Firefox : addons.mozilla.org/fr/firefox/addon/trashmailnet) ou encore dudmail.com.

# Cryptographie et chiffrement

La cryptographie est un des outils fondamentaux pour protéger son anonymat sur Internet. On l'a vu, les e-mails circulent sur Internet avec autant de sécurité qu'une carte postale. La cryptographie est donc un moyen efficace pour empêcher n'importe qui de lire ce que vous écrivez. Mais pas seulement.

« La cryptographie fonctionne. Des systèmes cryptographiques forts et correctement mis en place sont une des rares choses sur lesquelles il est possible de compter. » Ces mots sont d'Edward Snowden[163] : une telle confiance de la part d'un ancien agent de la NSA, voilà qui devrait convaincre les plus réfractaires de se mettre à la cryptographie.

## Qu'est-ce que la cryptographie ?

La cryptographie est l'art de réaliser une écriture secrète. C'est une technique ancienne, qui peut prendre plusieurs formes, mais a connu un véritable boom avec l'informatique et Internet, la mettant entre les mains de (presque) tous.

Pendant longtemps, la cryptographie était une arme. En France, elle était même interdite. Il est aujourd'hui absurde de la considérer comme telle, tant elle est présente partout sur Internet : tous les sites de e-commerce, de banques et, globalement, tous ceux qui manipulent des données sensibles y ont recours. La connexion en HTTPS (voir le chapitre 4) utilise ainsi une technique cryptographique ! Elle n'est plus l'apanage des geeks.

## Comment la cryptographie protège-t-elle les messages ?

La sécurité d'un message peut être définie par trois critères (déjà vus plus haut). En cryptographie, ces critères se déclinent sous trois noms : la confidentialité, l'intégrité, la non-répudiation.

- Confidentialité : cela signifie que le message reste privé. Le message chiffré ne peut être lu que par ceux qui disposent des clefs adéquates, des mots de passe et des outils nécessaires.
- Intégrité : cela veut dire que le message est le même au départ et à l'arrivée, qu'il n'a pas été altéré.
- Non-répudiation : cela signifie que l'on est sûr de la personne avec qui l'on échange, ou plus précisément qu'une personne ne peut pas démentir avoir envoyé un message.

En effet, beaucoup de solutions de cryptographie pour les e-mails comportent des solutions d'identification. C'est d'ailleurs un paradoxe que de parler de cryptographie dans cet ouvrage, puisque cette technologie facilite autant l'identification que l'anonymat. Elle ne protège en effet que l'un des composants de l'anonymat : le contenu du message (voir le chapitre 1). La cryptographie n'est donc pas l'anonymat : il faut la coupler avec d'autres techniques.

De plus, la cryptographie est un art difficile. Après avoir écrit les mots cités précédemment, Edward Snowden a ajouté : « Malheureusement, la sécurité aux extrémités de la communication est si terriblement faible que la NSA peut facilement la contourner. » L'ancien sous-traitant de la NSA met ici le doigt sur une des limites de la cryptographie : si tous les ordinateurs du monde ne suffisent pas à casser un message chiffré correctement, encore faut-il arriver à maîtriser les outils de chiffrement et le faire depuis des terminaux sécurisés. La cryptographie n'est décidément pas la panacée, mais seulement une partie – importante, certes – de la solution.

Au delà des e-mails, voici quelques conseils pour s'assurer du bon usage d'un outil ou d'un logiciel promettant de chiffrer vos communications de manière sécurisée :

- Le code est-il ouvert ? Cela permet de détecter les fonctionnalités dangereuses et/ou cachées : certaines entreprises comme Microsoft, lorsqu'elles découvrent des bogues, les communiquent d'abord et exclusivement aux autorités américaines[164], une dérive que peut éviter un code ouvert (voir chapitre 10).
- Est-ce que l'entreprise qui me fournit cette solution de cryptographie peut déchiffrer mes messages (ou est-ce moi seul qui détiens les clefs nécessaires) ? Dans le cas de Skype, par exemple, les conversations sont protégées, mais les gouvernements peuvent quand même demander à Skype de les déchiffrer.

**Noms Les personnages de la cryptographie**

Lorsque l'on parle de cryptographie, la coutume veut que l'on utilise toujours les mêmes prénoms : Alice et Bob sont les deux interlocuteurs qui veulent discuter en toute sécurité, Carol se joint parfois à eux, Eve est une espionne, Mallory et Oscar essaient de casser le chiffrement des messages entre Alice et Bob. Vous retrouverez ces prénoms dans de nombreux textes qui parlent de cryptographie.

## Vocabulaire de la cryptographie

Très tôt, les e-mails ont fait l'objet de recherches dans le domaine de la cryptographie. Philip Zimmerman a inventé PGP, un logiciel et une norme de cryptographie, depuis devenus le nom d'une entreprise qu'il a fondée.

On parlera surtout ici d'OpenPGP, la norme qui permet à différents produits d'utiliser cette technologie. Elle a l'avantage d'être libre (alors que PGP contenait des algorithmes propriétaires).

VOCABULAIRE **Chiffrer et crypter**

**Lorsque l'on protège un message à l'aide de la cryptographie, on le chiffre. Lorsque le correspondant le fait passer en clair (c'est-à-dire non chiffré), on dit qu'il le déchiffre. Crypter et ses variantes ne sont en fait pas français ! On conservera cependant le terme décrypter pour la technique qui consiste à casser le chiffrement.**

Vous entendrez parfois parler de GnuPG (ou GPG) : c'est un logiciel libre qui met en œuvre la norme OpenPGP. Pour l'usage et l'outil que nous avons retenus, vous n'aurez qu'à l'installer sur votre ordinateur.

## De quoi est constitué OpenPGP ?

Dans OpenPGP, il y a des algorithmes. Ce sont en quelque sorte les méthodes ou les formules mathématiques qui transforment un message en clair en message chiffré. Il y a deux types d'algorithmes de chiffrement :

- Symétrique : la même clef est utilisée pour chiffrer et déchiffrer. C'est le principe basique du A = 1, B = 2. Le problème avec ce type d'algorithme, c'est qu'il faut disposer d'un moyen de communication sûr pour échanger sa clef (sa méthode de chiffrement si vous préférez) en toute discrétion : si Mallory dispose de cette clef, elle peut lire tous les messages. Or, si on dispose d'un tel canal, pourquoi prendre la peine de tenter d'en créer un en chiffrant ?
- Asymétrique : un peu plus complexe puisque deux clefs différentes et complémentaires sont utilisées pour chiffrer et déchiffrer. Les systèmes cryptographiques asymétriques sont aussi dits « à clefs publiques » : une clef A vous appartenant est destinée à être partagée largement et sert à vos correspondants à chiffrer des messages qui vous sont destinés. Ces messages, vous ne pouvez les déchiffrer qu'avec votre clef

secrète, B. A et B sont appelées « paire de clefs ». C'est la solution utilisée par OpenPGP.

COMPRENDRE **Un cadenas ouvert et une clef**

Pour mieux comprendre le système de clef privée et de clef publique, on peut recourir à une image simple. C'est un petit peu comme si vous laissiez devant chez vous un casier avec un cadenas ouvert (la clef publique). Tout le monde peut mettre ce qu'il veut dans le casier et refermer le cadenas, mais seul vous, qui avez la clef du cadenas, êtes capable de le rouvrir (clef privée) et de voir ce qu'il y a dedans.

📖 *PGP et GPG : Assurer la confidentialité de ses e-mails et fichiers*, Michael W. Lucas, Eyrolles, 2006.

La confidentialité des échanges électroniques est de loin inférieure à celle du courrier postal et seul le chiffrement peut la garantir. Grâce à la norme OpenPGP et ses logiciels les plus connus, GnuPG et PGP, il est possible de chiffrer et signer ses e-mails et fichiers, que l'on soit sous Windows, Linux ou Mac OS X. Cet ouvrage explique simplement comment faire.

## Le système de clef privée et de clef publique

La longueur d'une clef se mesure en bits : plus il y en a, plus elle est difficile à casser (exemple : 128 bits, cela correspond à 340 sextillions de possibilités, soit 340 fois 10 puissance 34).

Une clef privée est composée de deux éléments. Le premier est tangible : c'est un fichier stocké (et même caché) sur votre disque dur. Le second est intangible (et doit absolument le rester) : la phrase de passe *(passphrase)*, qui sert à activer la clef, et qui doit être stockée uniquement dans votre mémoire. L'un ne fonctionne pas sans l'autre.

La clef publique (un simple fichier texte comportant des nombres et des signes), qui doit être accessible à vos correspondants, peut être soumise à ce que l'on appelle des « serveurs de clefs », des annuaires répertoriant les clefs publiques, comme keyserver.pgp.com ou pgp.mit.edu. Les logiciels utili-

sant OpenPGP peuvent ensuite aller chercher les clefs de vos correspondants directement sur ces serveurs. Il est aussi possible d'importer les clefs publiques de vos correspondants directement, sans passer par les serveurs. À une clef publique correspond(ent) une ou plusieurs adresses mail. Seule cette (ou ces) adresse(s) e-mail peu(ven)t fonctionner avec la clef publique associée.

**Conseil Les critères d'une bonne phrase de passe**

Une bonne phrase de passe doit être longue, facile à mémoriser, comporter des caractères spéciaux, des mots techniques, remplacer des lettres par des chiffres, être dans une langue étrangère. Cela peut être une réplique d'un film, d'une pièce de théâtre, des dictons ou des citations, tant qu'ils ne sont pas trop connus ! Exemple : la citation « celui qui croit qu'il n'a rien à cacher a déjà renoncé à sa liberté » du philosophe Wolfgang Sofsky peut devenir « c3|luiquin*r|3àcacheraD3j@ren0ncé&Sal-b3{té ». L'exercice est difficile, surtout qu'il faut éviter de conserver cette phrase ailleurs que dans sa mémoire, mais une bonne phrase de passe sera impossible à casser (ici, il faudrait qu'un ordinateur teste 106 puissance 42 possibilités, soit 106 suivi de plus de 40 zéros, pour la casser). Pour tout savoir des commandements du bon mot de passe, se reporter au chapitre 9.

## Générer sa clef

Lorsque vous débuterez avec OpenPGP, il vous faudra générer votre paire de clefs. Quelques conseils : il est souvent préférable de choisir une date d'expiration à sa clef pour la rendre inutilisable passé ce délai. On conseillera un an au débutant, un peu plus pour les utilisateurs confirmés. Il faut également penser à créer (et à stocker de manière très sûre) un certificat de révocation qui permettra, en le soumettant aux serveurs de clefs, de dire à tout le monde que la clef n'est plus active (parce qu'elle a été compromise par exemple).

Il est également intéressant de faire une copie de ses clefs, privée et publique (si votre ordinateur est dérobé ou doit être changé). Évidemment, il faut les stocker de manière sécurisée.

On voit bien ici pourquoi il ne faut pas stocker sa phrase de passe : si Mallory dispose de votre clef privée et de votre phrase de passe, tout est compromis.

PUBLIQUE **Comment diffuser sa clef publique ?**

Il y a plusieurs endroits où il est possible de diffuser votre clef publique : en signature de vos e-mails, sur votre site, sur des serveurs de clefs… Les deux premières solutions sont intéressantes du point de vue du propriétaire de la clef, moins du côté de celui qui la cherche : rien ne prouve que cette clef (et surtout l'adresse e-mail qui lui correspond) est bien celle du destinataire que vous voulez joindre. La troisième est également à prendre avec des pincettes puisque n'importe qui peut soumettre des clefs à un serveur de clefs. Le meilleur moyen est de la fournir en personne (à condition que votre interlocuteur soit digne de confiance, mais les capacités de la technologie s'arrêtent là où commencent les turpitudes humaines).

## Empreinte et signature

Comme évoqué plus haut, le système OpenPGP comporte également une forte dimension d'identification. Ne perdons pas de vue que la vie privée, c'est compartimenter et choisir qui a accès à quelle information. Savoir avec certitude avec qui vous discutez est donc un bon moyen de se protéger.

Une clef n'est pas franchement facile à lire. Imaginons qu'un ami vous demande de le contacter avec OpenPGP. Comment être sûr que la clef publique que vous allez utiliser est la bonne ? Demandez-lui, hors Internet, l'empreinte de sa clef. C'est une suite de dix fois quatre caractères, qui « résume » en quelque sorte la clef. Si un seul caractère de la clef change, l'empreinte est totalement différente. Les logiciels utilisant OpenPGP permettent d'afficher l'empreinte d'une clef que vous venez d'ajouter dans votre carnet d'adresses. Si l'empreinte de cette dernière est la même que celle que vous a fournie votre ami, tout est paré.

SIGNATURES **Le réseau de confiance**

Ce système de vérification de clef est utilisé dans le cadre du réseau de confiance. Celui-ci permet une utilisation fiable de OpenPGP : en signant publiquement la clef de quelqu'un dont vous êtes sûr de l'identité, vous indiquez à ses futurs correspondants que c'est bien lui qui utilise cette clef. Plus une clef est signée, plus elle est fiable. C'est ici un véritable système d'identification, plus que d'anonymat. Si vous souhaitez rester réellement indétectable, il faut bien sûr éviter de rentrer dans ce réseau de confiance. On peut cependant tout à fait imaginer que vous utilisiez deux adresses : l'une en dehors du réseau, l'autre à l'intérieur, en fonction de la nature de vos conversations.

## Signer ses messages

Il est également possible de vérifier l'intégrité du contenu du message : il suffit pour cela de signer ses messages. Concrètement, cela va ajouter un petit bout de code chiffré à la fin des messages envoyés. Votre correspondant va en vérifier l'authenticité en utilisant votre clef publique pour déchiffrer cette signature. S'il y parvient, c'est qu'il est bien la personne disposant de la clef privée correspondant à votre clef publique, qui a signé ce message.

À quoi cela sert-il si le message a été altéré ? C'est simple : la signature chiffrée au bas de votre e-mail contient en plus l'empreinte du message qui a été envoyé (comme plus haut, une sorte de résumé de votre message, qui change du tout au tout si un seul caractère a été modifié). Votre client calcule ensuite l'empreinte du message qu'il a reçu. Si les deux empreintes correspondent, cela signifie que le message n'a pas été altéré après avoir été signé par votre correspondant. Comme on ne peut signer un message qu'au moment où ce dernier est envoyé et que la signature est en pratique impossible à falsifier, vous avez, en plus de la confidentialité du message, l'assurance que vous discutez bien avec la bonne personne. Si votre client e-mail vous dit que tout va bien (généralement un petit message en vert au dessus de l'e-mail

reçu), cela signifie que le message n'a pas été altéré et que le bon destinataire vous l'a envoyé.

RÉSUMÉ **En quelques mots**

Si Alice veut envoyer un message à Bob, la clef privée d'Alice signe son message et la clef publique de Bob chiffre le message d'Alice. La clef privée de Bob déchiffre le message d'Alice et la clef publique d'Alice sert à vérifier que le message vient bien d'elle. Pour lire le message et vérifier son authenticité, il faut disposer de la clef publique d'Alice et de la clef privée de Bob. La seule personne disposant des deux est Bob.

## Chiffrer ses e-mails avec Enigmail

L'outil le plus simple à mettre en pratique pour chiffrer ses e-mails est très certainement Enigmail, compatible avec Thunderbird.

Thunderbird est l'équivalent de Firefox, mais pour les e-mails. Il est libre, gratuit, facile d'utilisation et disponible à la fois pour Mac, Linux et Windows. Nous recommandons fortement son utilisation si vous voulez chiffrer vos e-mails. Il existe bien évidemment des solutions différentes, mais si vous en connaissez, c'est que vous êtes déjà initié à la cryptographie et que vous n'avez certainement pas besoin de lire ce chapitre.

MAC **OpenPGP pour Apple Mail**

Il est possible de chiffrer ses messages avec le client e-mail fourni par Apple. Un bon tutoriel est disponible ici :

> hoylen.com/articles/it/email/security/mail.html

Une fois Thunderbird installé et votre compte e-mail configuré, il vous faut installer GnuPG (souvenez-vous, OpenPGP est une norme, GnuPG ou GPG le logiciel qui la fait fonc-

tionner). Vous pouvez télécharger ce dernier sur le site gpg4win.org.

Ensuite, il faut vous rendre dans le gestionnaire de modules complémentaires de Thunderbird (menu *option*) afin d'installer Enigmail. Une fois installée, l'extension est simple à mettre en pratique.

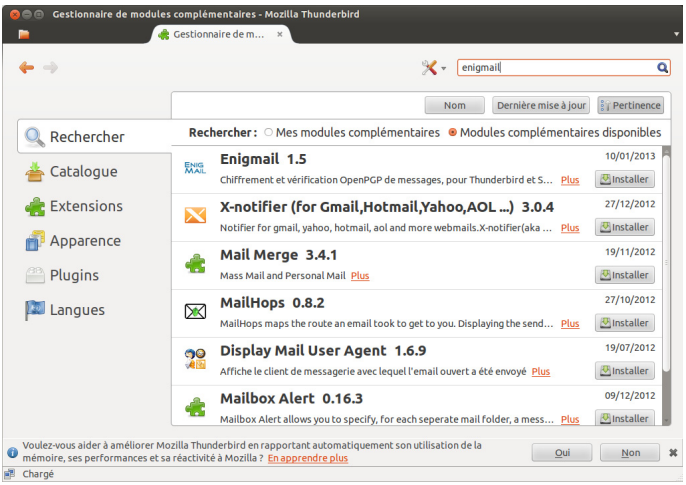



**Fig. 6–2 > L'écran du gestionnaire d'extension de Thunderbird lorsque l'on y recherche Enigmail.**

## Créer sa clef

Il faut d'abord générer une paire de clefs. Pour cela, il faut aller dans le menu *OpenPGP* – qui doit apparaître dans la barre de menus de Thunderbird maintenant qu'Enigmail est installé – puis dans le sous-menu *Gestion de clefs* et enfin dans le menu *Générer une nouvelle paire de clefs*. Le menu suivant (figure 6-3) doit apparaître.

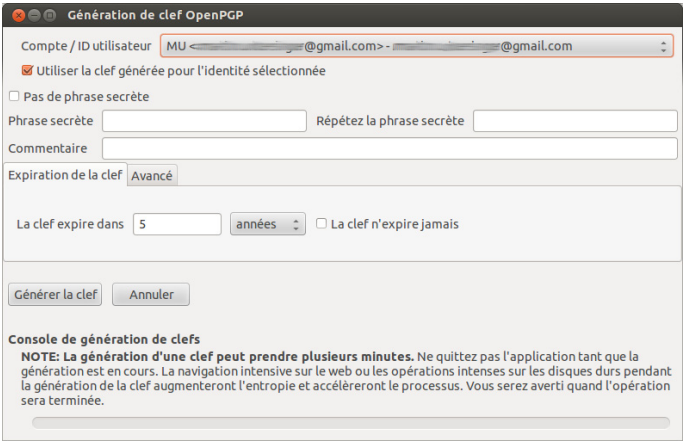



Fig. 6–3 > L'écran de génération de clef

Après avoir entré une phrase secrète (phrase de passe) et réglé la durée d'expiration des clefs, cliquer sur *Générer la clef*. Pour augmenter l'entropie, c'est-à-dire le caractère aléatoire de ces clefs, il est conseillé d'utiliser son ordinateur pendant les quelques minutes que prend le processus de génération. Cela accroît la sécurité.

### Nouveauté Chiffrer avec PGP depuis son navigateur

Il est théoriquement possible d'installer une extension sur son navigateur pour chiffrer ses e-mails Gmail par exemple, en s'économisant l'installation laborieuse de Thunderbird et Enigmail. Google a tout récemment publié le code d'une extension qu'il espère un jour proposer au grand public[165]. Ce n'est pas la première initiative du genre et, pour le moment, personne n'est parvenu à une solution acceptable en termes de sécurité, notamment en raison des limites du langage utilisé (JavaScript) en matière de cryptographie. C'est donc à éviter pour le moment.

Il faut ensuite générer le certificat de révocation lorsque le logiciel le propose. Ensuite, vous êtes à nouveau sur l'interface de *Gestion des clefs*. Votre clef n'apparaît pas ? C'est normal, le logiciel n'affiche pas par défaut les clefs qu'il a enregistrées. En revanche, si vous saisissez les premiers caractères de votre adresse e-mail dans le champ de recherche, votre paire de clefs devrait apparaître. Avec un clic-droit, il est possible de faire apparaître les options de la clef.

## Envoyer la clef sur le serveur

Pour que vos correspondants puissent trouver votre clef, il vous faut l'envoyer sur des serveurs dédiés. Pour cela, il faut cliquer sur *Envoyer les clefs publiques vers un serveur de clefs*. Il est également possible d'envoyer votre clef publique directement depuis le site web du serveur de clefs.

En pratique, tout le monde peut poster une clef. On pourrait penser que cela pose problème, mais en réalité seule la signature (combinaison clef publique/clef privée) peut authentifier un destinataire. L'usage veut cependant qu'on ne publie sur un serveur de clefs que ses propres clefs.

Pour récupérer les clefs d'un correspondant, il est possible de laisser Enigmail s'en occuper ou d'aller les chercher soi-même. Une bonne méthode consiste à copier la clef, puis à utiliser le menu d'OpenPGP intitulé *Copier une clef depuis le presse papier*. Et voilà, la clef de votre correspondant est ajoutée à votre trousseau et sera utilisée automatiquement lorsque vous écrirez à ce correspondant.

**Recherche Comment trouver la clef PGP de vos correspondants ?**

Depuis Thunderbird, Enigmail peut aller chercher, automatiquement, sur plusieurs serveurs de clefs celle de votre correspondant. Si vous voulez la chercher à la main, c'est également possible : subkeys.pgp.net, keyserver.pgp.com, pgp.mit.edu sont des serveurs de clefs réputés. keyserver.pgp.com a l'avantage d'envoyer un e-mail de confirmation pour vérifier que c'est bien son propriétaire qui lui a soumis sa clef.


Fig. 6–4 > Sélectionner le serveur de clefs

## Stocker ses clefs

Il est ensuite souhaitable de faire une sauvegarde de sécurité de votre paire de clefs. Pour cela, cliquez-droit sur la clef puis choisissez *Exporter les clefs vers un fichier*, en pensant à sélectionner également la clef privée.

## Envoyer un message chiffré et signé

Lorsque vous rédigez un message (et que vous avez ajouté la clef publique de votre destinataire à votre trousseau), il suffit de cliquer sur le menu *OpenPGP* et de sélectionner les options *Chiffrer le message* et *Signer le message*. Le message sera chiffré lorsque vous l'enverrez (Enigmail vous demandera votre phrase de passe).

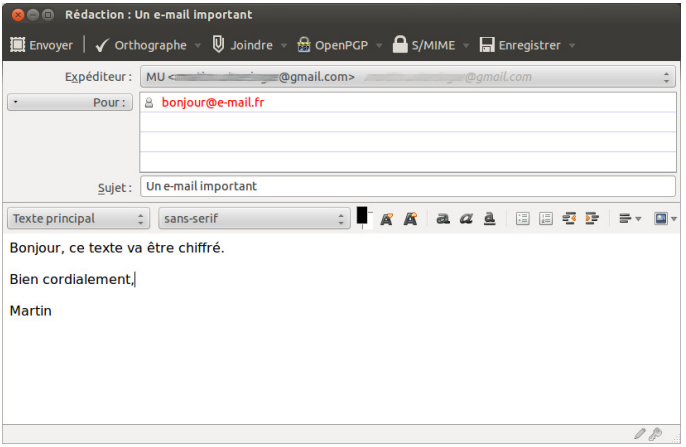



**Fig. 6–5 > L'écran de saisie de l'e-mail chiffré, avec le symbole OpenPGP en haut**

Lorsque vous recevez un message chiffré, il vous faut simplement cliquer sur ce même bouton pour déchiffrer et vérifier la signature. S'il n'y a pas d'erreur, vous pourrez lire le message. Si Enigmail vous affiche un message d'erreur quant à la signature de votre correspondant, méfiez-vous !

**Attention Ce qui n'est jamais chiffré dans un e-mail**

L'objet de l'e-mail et les deux adresses des protagonistes ne sont jamais chiffrés. Plus généralement, toutes les données annexes de l'e-mail, qu'on appelle le *header* (l'en-tête), circulent en clair.

## Les problèmes posés par OpenPGP

Le premier problème d'OpenPGP, et presque le seul, est sa grande complexité. Une fois que vous aurez compris et pratiqué, cela passera comme une lettre à la poste (en plus sûr). Avant cela, vous êtes susceptible de mal maîtriser la techno-

logie et donc de faire des erreurs en vous pensant en sécurité (choisir une phrase de passe trop faible, stocker votre clef privée dans un lieu accessible). C'est sans compter le fait que votre interlocuteur est également responsable de votre sécurité : il faut donc être deux à parfaitement maîtriser la technique et les outils. Or, rien n'est pire qu'un faux sentiment de sécurité. N'hésitez donc pas à vous exercer avec des amis, sans enjeu : le jour où vous en aurez vraiment besoin, cela se passera sans problème.

### Problème Le stockage des messages

**Quand Alice envoie un message à Bob, ce message ne peut être lu qu'avec la clef privée de Bob. Or, Alice ne dispose pas de cette clef : elle ne peut donc pas lire le message qu'elle a envoyé (sauf si son logiciel de messagerie conserve le message en clair). Du coup, son message n'est pas protégé sur son disque dur. On peut aussi chiffrer les messages qu'on envoie avec sa propre clef publique à des fins de sauvegarde, pour les conserver chiffrés dans son logiciel de messagerie, mais cela demande un peu de temps supplémentaire.**

Cette technologie n'offre pas une protection absolue, mais elle est formidablement difficile à contourner. Personne n'y est jamais parvenu. Pour autant, cela ne veut pas dire que votre anonymat soit protégé de manière absolue : votre adversaire choisira une autre technique d'attaque.

Il pourra par exemple choisir une faille de sécurité bien plus « basique » : si une personne a physiquement accès à votre ordinateur, si ce dernier est mal protégé par mot de passe, elle pourra accéder à vos archives d'e-mails. Elle pourra également utiliser un *keylogger* (un programme qui surveille et diffuse les touches que vous pressez au clavier, pour repérer votre clef privée ou le contenu des messages que vous tapez), ou procéder au vol de votre disque dur dans lequel est enregistrée votre clef privée.

**Choix Plusieurs clefs, un même nom**

En cherchant les clefs publiques d'un correspondant potentiel, il se peut que vous tombiez sur plusieurs clefs. Tout d'abord, cela peut vouloir dire que le correspondant ne maîtrise pas forcément parfaitement OpenPGP (qu'il a perdu sa phrase de passe, sa clef privée ou qu'il n'a pas su émettre de certificat de révocation) : prudence, donc. Comment savoir quelle clef est la bonne ? Il faut déjà resserrer votre recherche sur les clefs qui sont encore valides. Ensuite, celle qui est la plus récente est celle qui a le plus de chances d'être encore valide. On peut alors se servir du réseau de confiance et regarder celle qui est le plus signée. On peut également aller voir sur les sites personnel, professionnel ou les réseaux sociaux de la personne que l'on cherche à joindre : elle y a peut-être laissé sa bonne clef publique.

Dans un monde idéal, tout le monde chiffrerait ses e-mails. Mais voilà, si vous cherchez à camoufler votre activité à un gouvernement ou à des gens ayant des moyens importants, vous voir échanger des e-mails chiffrés ou en trouver l'archive sur votre disque dur peut les convaincre que vous tramez quelque chose (même si ce n'est pas le cas). En ce sens, chiffrer peut attirer l'attention. Une solution peut être de supprimer systématiquement les e-mails reçus après réception (et d'utiliser le protocole POP3).

Bien sûr, l'erreur humaine n'est jamais loin : ne donnez (ni n'oubliez) jamais votre phrase de passe, vérifiez toujours les signatures de vos correspondants…

## Le chiffrement ne suffit pas

Le chiffrement n'est pas l'anonymat, c'en est une composante. Envoyer un e-mail avec votre adresse prenom.nom@gmail.com, ce n'est pas être anonyme : malgré le chiffrement, les adresses e-mails des correspondants apparaissent en clair. Une solution peut être d'utiliser un compte e-mail parfaitement anonyme (voir plus haut).

Parfois, sans même savoir qui échange quoi et avec qui, les seules dates, tailles et fréquences des discussions peuvent en dire beaucoup sur l'identité des protagonistes.

De plus en plus d'entreprises proposent des solutions de chiffrement d'e-mails. On notera la création de Silent Circle, dont Philip Zimmerman, l'inventeur de PGP, est un des cofondateurs[166].

Même si leur technologie est trop récente pour avoir du recul, voici quelques éléments, à la fois négatifs et positifs, à garder en tête :

- Ils gardent les logs (https://silentcircle.com/web/privacy/) de connexion.
- Leur méthode de chiffrement a l'air fiable.
- Ils répondront au gouvernement, mais jouent la transparence en s'engageant à publier un rapport détaillé, chaque année, sur demande.
- Leur infrastructure n'est pas centralisée, mais en peer-to-peer.
- Leur entreprise se situe hors de la juridiction américaine : leur infrastructure est au Canada[167].
- Le service est payant.
- Ils songent à mettre à l'avenir leur logiciel en open source.

## Messagerie instantanée

Le chat est un moyen pratique et rapide de communiquer sur Internet. Cependant, comme pour les e-mails ou la navigation sur le Web, les messages envoyés transitent par plusieurs serveurs, tous susceptibles d'en conserver des copies. Sans compter le risque que quelqu'un surveille les échanges entre votre machine et celle de votre interlocuteur, ou celui que la fonctionnalité d'archive de discussion de votre logiciel de chat et/ou de celui de votre correspondant conserve des copies de

vos précieuses discussions. Heureusement, un chat est souvent plus facile à sécuriser qu'un e-mail.

D'abord, précisons un peu de vocabulaire. Il y a deux éléments dans le chat. Le premier est le protocole, c'est-à-dire le langage que les machines doivent parler pour se comprendre. Il est important de connaître quel protocole vous voulez utiliser (ou utilisez déjà), parce qu'ils n'ont pas tous les mêmes garanties en termes de sécurité. Le second élément est le client, le logiciel qui va parler ce langage et qui est utilisé pour recevoir et envoyer des messages.

On distingue généralement deux types de protocoles : les protocoles ouverts et les protocoles fermés. La différence entre les deux est simple.

Le fonctionnement des protocoles ouverts est largement documenté, ce qui permet de développer facilement de nouveaux clients. Le protocole fermé, ou propriétaire, signifie que seule l'entreprise qui le développe sait parfaitement comment il fonctionne et, au final, votre capacité à interagir avec vos correspondants reste entre ses mains (ainsi que les données que vous envoyez sur le réseau, ce qui peut poser problème si vous ne chiffrez pas vos communications).

Parmi les protocoles ouverts, on citera XMPP (anciennement Jabber) ou IRC. Les protocoles fermés sont les plus connus : ICQ, AIM, Skype (ex-Windows Live Messenger).

Évidemment, dans une optique de sécurité et d'anonymat, il faut privilégier les protocoles ouverts.

Tout ceci est un peu abstrait, précisons-le donc. Pour utiliser une messagerie instantanée XMPP, il faut se créer un compte sur un serveur qui utilise le protocole XMPP. Vous l'avez sans doute déjà fait puisque Google et Facebook utilisent ce protocole : le XMPP est la technologie qui fait fonctionner leurs messageries instantanées. Cela ne veut pas pour autant dire que l'utilisation du chat Google ou Facebook est sans

danger, puisque toutes les communications transitent (et sont éventuellement stockées et analysées) sur leurs serveurs.

Néanmoins, il est tout à fait possible d'utiliser XMPP sans passer par Google. On recommandera par exemple le serveur du Chaos Computer Club allemand : jabber.ccc.de. Le CCC est un légendaire groupe de hackers qui se bat depuis des années pour la vie privée sur les réseaux. À ce titre, l'auteur de ces lignes les considère dignes de confiance (mais c'est un calcul que vous vous devez de faire, et pas uniquement pour choisir votre serveur de chat). Il faut noter qu'ils conservent quand même quelques informations, notamment la date de création du compte[168].

Nous tendons à recommander l'utilisation de XMPP pour vos discussions sécurisées, mais IRC est également un choix tout à fait valable. Les avantages de XMPP sont les suivants :

- Large compatibilité : vous pourrez discuter avec vos amis qui utilisent Gmail (mais si vous ne chiffrez pas vos télécommunications, les messages seront vus par Google, même si vous n'utilisez pas Google vous-même). Contrairement à IRC, on peut dialoguer avec des comptes XMPP qui ne sont pas inscrits sur un même serveur.
- Il est assez complet puisqu'il permet de gérer des contacts, un avatar, une carte de visite, la discussion de groupe et le transfert de fichiers.
- Il est décentralisé. Le protocole XMPP ne dépend donc pas d'une entreprise (ou d'un serveur) en particulier.
- En revanche, si le serveur que vous utilisez tombe en panne ou entre des mains peu amènes, vous ne pourrez rien faire, sinon chiffrer vos communications.

Les clients sont pour la plupart compatibles XMPP (également IRC).

En termes de clients, si vous utilisez Linux ou Windows, Pidgin est extrêmement performant, sécurisé, libre et simple

d'utilisation. Adium, uniquement sur Mac, est également très recommandable. Il en existe d'autres comme Kopete (Linux) ou Mumble (Windows, Mac, Linux).

**Mémo Pensez à désactiver l'historique des chats !**

Souvent, votre client de chat (ou le compte e-mail que vous utilisez pour « chatter », comme Google) conserve un historique des conversations, ce qui peut être embêtant du point de vue de la confidentialité. Il est possible de désactiver cette fonction dans les paramètres du client (si vous utilisez Gmail par exemple, il faudra également le désactiver dans vos paramètres Gmail).

## Chiffrer vos discussions instantanées avec OTR

La solution la plus pratique pour sécuriser vos chats est d'utiliser la technique OTR (Off the Record).

**Difficile GPG pour les conversations instantanées**

Il est également possible d'utiliser GPG pour sécuriser ses conversations instantanées. Toutefois, son utilisation est un peu plus compliquée. Il est préférable de bien apprendre à vous servir d'OTR (et aussi, surtout, d'expliquer à vos correspondants comment faire de même) et par ailleurs de maîtriser GPG pour vos e-mails, ce qui n'est pas une mince affaire. Car souvenez-vous : rien n'est pire qu'un outil de sécurité mal paramétré ou mal maîtrisé. Il vous fourvoie dans un faux sentiment de sécurité. Si toutefois l'aventure GPG pour messagerie instantanée vous tente, Internet compte plusieurs tutoriels très bien faits. Il est également possible de configurer son client de chat pour qu'il utilise Tor, pour davantage encore de sécurité (voir le chapitre 7).

OTR s'installe très simplement, sous la forme d'une extension (parfois appelée « hors micro » en français). Elle est même parfois déjà installée. Si tel n'est pas le cas, elle est téléchargeable sur cypherpunks.ca/otr/#downloads. Attention, cette fonctionnalité doit également être activée chez votre correspondant.

Lorsque c'est le cas et qu'une nouvelle discussion débute, un message signalant le début d'une conversation privée apparaît. Si ce n'est pas le cas, il est possible de forcer le démarrage de la conversation, généralement au moyen d'un bouton. À la fin de la discussion, il est plus sûr de terminer la conversation privée, surtout lorsqu'un des deux correspondants s'est déconnecté.

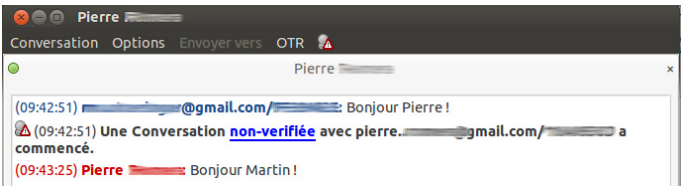



FIG. 6–6 > Le début d'une conversation privée (Pidgin)

Les messages que vous envoyez dans le cadre d'une conversation protégée par OTR sont chiffrés, ce qui signifie qu'il est très difficile pour une tierce personne de savoir ce que vous écrivez. De plus, les extensions OTR disposent d'options permettant d'identifier votre correspondant, afin d'être sûr de la personne avec qui vous correspondez (comme PGP !). Généralement, il y a trois moyens de le faire :

- une question secrète (si vous fournissez tous les deux la bonne réponse, c'est gagné) ;
- un secret partagé (si vous saisissez le même mot ou la même phrase, c'est aussi gagné) ;
- la vérification d'empreinte (mais il faut alors se communiquer l'empreinte par un autre canal sécurisé).

Attention, même chiffrée, une conversation privée OTR ne protège pas l'identité de la personne avec qui vous conversez (comme les e-mails chiffrés).

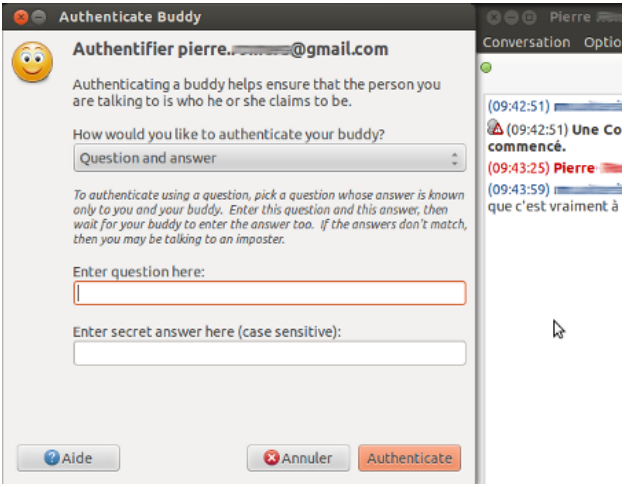



FIG. 6–7 > L'écran de saisie de la question secrète

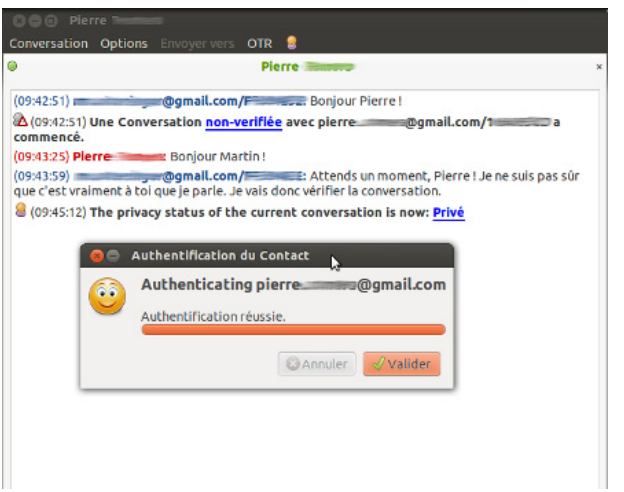



FIG. 6–8 > L'identification a été correctement effectuée.

### Détail Bien s'assurer d'être connecté en TLS/SSL

**En théorie, les dernières versions d'Adium et de Pidgin configurent automatiquement les comptes que vous ajoutez pour qu'ils utilisent TLS/SSL (voir le chapitre 4), ce qui procure un niveau de sécurité supplémentaire. Pour vérifier que c'est bien le cas, il faut se rendre dans les paramètres du compte (ou de vos comptes). Dans Pidgin, le réglage se trouve dans l'onglet *Avancé*, dans Adium, simplement dans les options.**

Les discussions instantanées posent un enjeu similaire aux e-mails : votre sécurité ne dépend pas seulement de vous, mais également des précautions que prend votre interlocuteur (par exemple, s'il stocke vos conversations alors que vous estimez que c'est risqué).

De nombreuses applications ou services vous promettent des solutions de discussions confidentielles et/ou chiffrées. Elles ne sont pour la plupart pas auditées par des professionnels de manière fiable. On conseillera donc de rester fidèle au duo chat XMPP + OTR, qui offre une robustesse inégalée en termes de sécurité.

Cependant, une application mérite le détour : il s'agit de Cryptocat[169], qui se présente sous la forme d'une extension pour la plupart des navigateurs (Chrome, Firefox, Safari, Opera...). Open source (et audité à plusieurs reprises), il implémente OTR de manière très simple pour l'usager et assure ne pas collecter d'informations identifiantes. On peut considérer ce service comme globalement fiable et très adapté à de faibles menaces. Une application pour iOS est également disponible.

# Discuter en son et en images : la voix sur IP (VOIP)

La VOIP (ou voix sur IP), c'est-à-dire la conversation utilisant le son (et la vidéo) sur Internet, s'est fortement développée ces dernières années, notamment grâce au succès du logiciel Skype.

Attention, Skype est une entreprise privée (rachetée par Microsoft) et donc fermée ; il n'est pas très prudent de lui faire confiance pour une discussion véritablement anonyme et privée. Cela dit, il est possible de minimiser les dégâts en créant un compte depuis le site de Skype, abrité derrière un VPN (voir le chapitre 7) et de fournir à l'entreprise des informations erronées et une fausse adresse e-mail (voir précédemment).

Le problème est que Skype est l'objet d'une véritable controverse au sein des spécialistes de la sécurité. S'opposent d'un côté, ceux qui reprochent à Skype son opacité, notamment vis-à-vis des requêtes que l'entreprise reçoit de la part des gouvernements et de l'autre, ceux qui estiment que Skype est une solution suffisamment sécurisée pour un certain nombre d'usages.

FERMÉ **Skype, complètement opaque**

**En plus d'avoir un code fermé et non open source, ce qui rend le développement de logiciels compatibles impossibles, le *reverse engineering* (technique consistant à désosser un logiciel pour voir comment il fonctionne) s'applique très difficilement à Skype. Bref, on n'en connaît pas grand-chose et ce n'est jamais bon en sécurité informatique.**

Skype chiffre toutes les communications. Cela veut dire qu'en théorie, il est difficile pour une tierce personne d'écouter ce que disent deux interlocuteurs sur le service. De plus, son architecture est basée sur le peer-to-peer, ce qui signifie que les communications ne passent pas par un seul serveur central.

Pendant longtemps, Skype a été réputé pour sa grande sécurité[170].

Cependant, comme le code source de Skype est fermé, il est impossible de savoir ce que le logiciel fait réellement sur votre ordinateur. De plus, du fait de son architecture en pair à pair, le trafic d'autres usagers peut emprunter votre machine, ce qui pose problème si on ne sait pas exactement ce qui se trame dans le logiciel.

De plus, des chercheurs ont montré qu'il était assez facile techniquement d'accéder aux adresses IP des internautes utilisant Skype et d'accéder à des informations telles que leur localisation ou leur activité sur le réseau[171]. Autre alerte : après avoir racheté Skype, Microsoft a acquis un brevet permettant d'intercepter et de copier des conversations VOIP. Aujourd'hui, Skype ne veut pas dire si oui ou non cette technique est employée par son logiciel[172]. Dans certains pays, notamment la Syrie, le gouvernement aurait mis en place des logiciels espions interceptant les communications de Skype avant qu'elles ne soient chiffrées[173], ce qui aurait déjà coûté la vie à plusieurs personnes.

Par ailleurs, les documents soustraits à la NSA par Edward Snowden montrent que Skype fait partie du programme Prism, qui donne à l'agence un accès privilégié à ses données.

Enfin, le chiffrement n'est pas l'anonymat. Comme dans le cas des e-mails et des chats, il est possible pour Skype, et donc pour les gouvernements qui lui en feraient la demande, de savoir qui a parlé à qui, quand et pendant combien de temps, ce qui suffit pour poser potentiellement de graves problèmes. Bref, Skype semble rester sécurisé pour des conversations peu sensibles. Pour le reste, il faudra se contenter des e-mails, ou d'une conversation hors Internet.

Les solutions alternatives à Skype sont pour le moment rares. Silent Circle (voir plus haut), en propose une, ainsi que Jitsi.org.

Pour une solution permettant uniquement l'utilisation du son (et pas de la vidéo), on privilégiera le logiciel libre Mumble.

## L'erreur humaine

Pour conclure ce chapitre, on rappellera qu'en matière de sécurité informatique, on est toujours à la merci d'une erreur humaine : il suffit d'une négligence (se connecter sans son VPN, oublier son ordinateur non protégé ou se connecter à un réseau Wi-Fi d'aéroport) et toute votre stratégie de protection de l'anonymat peut voler en éclats.

De plus, toutes les techniques que nous avons vues ne concernent que des communications, c'est-à-dire entre votre machine ou appareil et celui ou celle de votre interlocuteur. Il existe des menaces directement sur votre ordinateur, qui peuvent espionner votre activité et vos communications, même si ces dernières sont protégées par les techniques présentées (keyloggers – programmes qui enregistrent les touches frappées sur votre clavier –, trojans, virus…). Enfin, que ce soit pour un compte e-mail, chat ou autre, il vous faudra toujours utiliser des mots de passe à toute épreuve (voir le chapitre 9).

# 7 Protéger sa connexion : proxies, VPN et le projet Tor

*Nous abordons à présent la partie la plus technique de cet ouvrage, qui va vous apprendre à camoufler votre connexion et notamment votre adresse IP.*

## Les proxies

Souvent, lorsqu'on évoque la question de l'anonymat sur Internet, on évoque la solution des proxies. Elle peut en effet être considérée, mais les dangers et les limites sont nombreux.

## Les proxies, comment ça marche ?

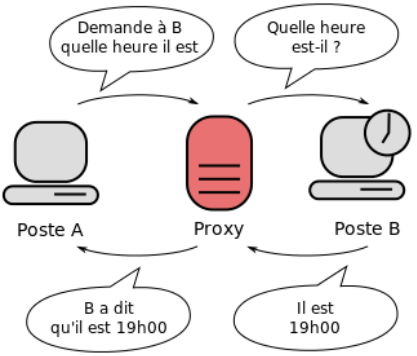



FIG. 7–1 > Fonctionnement d'un serveur proxy (Wikimedia CC BY-SA 3.0)

Un proxy (parfois désigné, en bon français, par « serveur mandataire ») est un terme très générique. Il s'agit d'un ordinateur tiers à travers lequel vous accédez à un service Internet. Il fonctionne comme une sorte de tampon entre un ordinateur et un site web. La connexion issue de l'ordinateur transite d'abord par le proxy avant d'atteindre sa cible.

Il existe de nombreux types de proxies (sur Internet, ils se comptent par milliers), qui offrent tous des fonctionnalités et des niveaux de protection différents. Le principal avantage dans le cas d'un proxy utilisé pour l'anonymat, c'est que le site cible ne peut pas connaître votre adresse IP réelle : c'est celle du proxy qui lui parvient.

## Limitations du proxy

Cette technologie n'offre qu'une protection extrêmement relative.

Votre connexion Internet n'étant pas chiffrée sur tous les proxies, votre fournisseur d'accès à Internet continue de voir tout ce que vous faites sur le réseau. Le proxy lui-même peut voir tout ce que vous faites avec votre connexion.

Tous les proxies ne comportent pas les mêmes fonctionnalités protégeant l'anonymat. Certains vont rendre par exemple votre adresse IP accessible indirectement aux sites que vous visitez.

### Conseil Les proxies, une utilisation à limiter

L'anonymat n'est qu'une des utilisations possibles d'un proxy, qui peut également servir, par exemple, à contourner le blocage de sites web. S'il est nécessaire pour vous d'adopter une protection forte, on recommandera plutôt l'utilisation d'un VPN ou de Tor (voir plus loin).

Si on raisonne en termes d'anonymat, il existe trois types de proxies :

- Les proxies transparents : l'adresse IP est visible pour le proxy et pour le site visité, car elle est présente dans la requête HTTP qui est faite pour accéder au site.
- Les proxies anonymes : l'adresse IP est visible, mais un peu plus difficile d'accès.
- Les proxies hautement anonymes : l'adresse IP n'est pas visible.

Pour savoir quel niveau de protection offre un proxy, il n'y a pas beaucoup de solutions, sinon de faire quelques tests et de chercher sur Internet les proxies réputés les plus sûrs.

### Pratique Voir ce qui est transmis dans l'en-tête HTTP

À chaque fois que votre navigateur va sur une page web, il transmet un certain nombre d'informations, dont votre adresse IP, dans ce qu'on appelle l'en-tête HTTP. Pour vérifier que le proxy que vous utilisez la dissimule correctement, vous pouvez faire un test en vous rendant, à travers le proxy, sur xhaus.com/headers.

## Les proxies web, HTTP et SOCKS

Techniquement, on s'attardera sur deux types de proxies : les proxies web et les proxies HTTP.

Les proxies web s'utilisent simplement depuis un navigateur et se présentent comme une simple page web, dans laquelle il est possible de saisir une autre adresse, celle à laquelle vous voulez accéder à travers le proxy.

Ils sont très basiques puisqu'ils ne permettent pas l'utilisation de plusieurs applications (e-mails, discussions instantanées), mais uniquement de consulter des pages web.

### En pratique Quelques annuaires de proxies web

> publicproxyservers.com/index.html
> samair.ru/proxy
> listeproxy.net
> free-proxy.fr
> proxy4free.com
> googlebig.com/sections/Googlebig-Http-Proxy

Le deuxième type de proxy est appelé HTTP (ou parfois HTTPS, plus sécurisé). Il fonctionne de la même manière, sauf qu'au lieu de l'utiliser via une page web, il est accessible en modifiant les paramètres de l'application (navigateur, client e-mail…) : il faut alors y renseigner l'adresse IP du proxy.

Il existe un troisième type de proxy, appelé SOCKS, qui est assez similaire aux proxies HTTP – notamment dans leur configuration –, mais qui permet l'utilisation d'un plus grand nombre de logiciels et d'applications.

EN PRATIQUE **Annuaires de proxies HTTP et SOCKS**

> hidemyass.com/proxy-list
> web.freerk.com/proxylist.htm
> proxies.by/proxy

Certains sites listent les proxies en précisent la nature (HTTP, SOCKS), mais également le niveau de sécurité.

Qu'ils soient HTTP ou web, les proxies sont généralement dits ouverts, c'est-à-dire qu'ils peuvent être utilisés gratuitement par n'importe qui. Leur utilisation n'est pas du tout recommandée dans une optique d'anonymat, car on ne sait jamais vraiment comment ils ont été configurés, s'ils sont dignes de confiance, surveillés ou pas… Un proxy peut être utile pour contourner le blocage ou le filtrage, mais pas pour un anonymat robuste et durable.

## Comment utiliser un proxy ?

Les proxies fournis par ces sites sont de la forme suivante : une adresse IP (par exemple 123.45.6.7) et un numéro de port (c'est-à-dire la porte que va emprunter votre connexion sur le serveur proxy et qui peut être n'importe quel nombre). Parfois, les deux seront accolés, comme ceci : 123.45.6.7:8080.

PRÉCAUTION **Essayer de toujours chiffrer sa connexion**

Si vous utilisez un proxy, votre connexion ne sera normalement pas chiffrée et votre fournisseur d'accès à Internet ainsi que le proxy utilisé pourront voir votre activité en ligne. L'utilisation d'un proxy ne dispense absolument pas de l'utilisation des outils et des précautions abordés dans le chapitre 5, notamment le plug-in HTTPS everywhere et les anti-traceurs.

Muni de ces deux informations, vous pouvez paramétrer votre navigateur ou votre client d'e-mail ou de discussion instantanée. Dans Firefox, il faut se rendre dans les paramètres avancés, puis dans l'onglet *Réseau* et cliquer sur le bouton *Paramètres* dans *Connexion*.

Après avoir coché *Configuration manuelle du proxy*, il faut simplement entrer l'adresse IP et le port du proxy désirés dans les champs correspondants (HTTP ou SOCKS, selon le type). Dans les autres navigateurs, la manipulation est sensiblement la même. Une fois ces paramètres activés, il est conseillé de redémarrer son navigateur pour plus de sécurité.

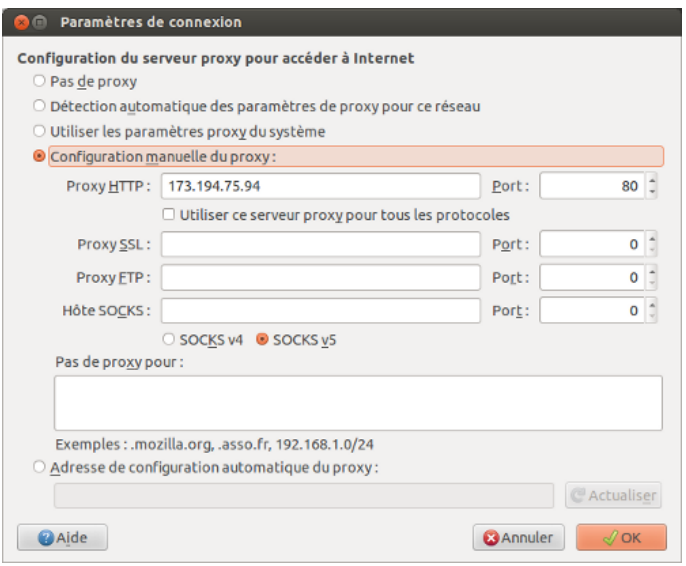



**Fig. 7–2 > Comment configurer Firefox pour qu'il utilise un proxy.**

Ce type de configuration par le navigateur pose un problème : on ne peut pas forcément l'utiliser sur des ordinateurs sur lesquels on n'a pas de privilèges d'administrateur.

EN PRATIQUE **Une connexion plus lente**

**Notez que si vous utilisez un proxy, votre navigation sera nécessairement plus lente, puisqu'elle devra emprunter une étape supplémentaire.**

## Logiciels et extensions pour gérer les proxies

Il existe certaines extensions gérant plus efficacement la connexion à plusieurs proxies :

- IPflood (addons.mozilla.org/fr/firefox/addon/ipflood) ;
- Elite Proxy Switcher (addons.mozilla.org/en-US/firefox/addon/elite-proxy-switcher) ;
- FoxyProxy (getfoxyproxy.org).

Les logiciels de serveurs proxies peuvent être installés par quelqu'un en qui on a confiance sur son propre serveur. Il faut ensuite paramétrer ses applications pour y accéder. Si vous connaissez quelqu'un qui dispose de son propre serveur et est prêt à vous aider, il est possible de lui demander d'installer ce type de technologie.

ASTUCE **Changer régulièrement de proxy**

**Si vous deviez choisir un proxy pour vous protéger (ce n'est pas très recommandé), il est conseillé d'utiliser des proxies populaires dans sa région et d'en changer régulièrement. Bref, agir un peu comme lorsqu'on est poursuivi : se fondre dans la foule et bouger tout le temps.**

Même si les proxies peuvent être intéressants ponctuellement, pour contourner un blocage par pays ou pour dissimuler de manière légère son adresse IP, il ne faut pas qu'ils soient utilisés pour une anonymisation importante. Pour cela, il faut privilégier d'autres technologies, comme les VPN.

# Les réseaux privés virtuels ou VPN

Les réseaux privés virtuels, ou VPN, font partie des outils délicats à maîtriser parfaitement. Ils sont destinés à ceux qui veulent protéger leur connexion sur une longue période de temps (pour travailler, par exemple).

Pour ceux qui souhaiteraient une protection plus forte encore mais plus ponctuelle, on recommandera l'utilisation de Tor (voir plus loin).

## Qu'est-ce qu'un VPN et comment marche-t-il ?

Un VPN (*Virtual Private Network*, réseau privé virtuel) est un tunnel entre deux machines utilisé pour dissimuler les données qui y transitent et camoufler l'identité de l'utilisateur à un regard extérieur (notamment celui de son fournisseur d'accès à Internet). C'est tout simplement un réseau privé qui utilise un réseau public (Internet) : votre ordinateur est relié à un autre, de manière confidentielle.

Les données sont envoyées chiffrées au VPN, de telle sorte qu'il est impossible de voir ce qui se passe dans la connexion. Ensuite, les VPN dont nous allons aborder le fonctionnement servent généralement d'intermédiaire, à la manière d'un proxy, vers le site ou le service que vous voulez visiter. De cette façon, le site cible voit arriver une connexion qui possède l'adresse IP du VPN, mais ne voit jamais la vôtre.

Il existe des VPN gratuits, mais les services payants (souvent entre cinq et dix euros par mois) sont plus fiables, plus rapides, moins susceptibles de garder une trace de votre connexion et d'afficher des publicités.

Une fois que vous êtes inscrit et que votre abonnement est validé, le fournisseur de VPN vous envoie les détails nécessaires à la configuration de vos logiciels. Il s'agit notamment d'un nom d'utilisateur, que vous choisissez le plus souvent, et d'un

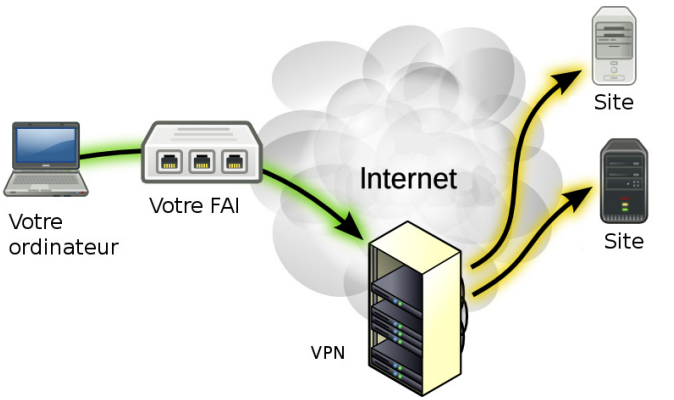



FIG. 7–3 > Schéma de fonctionnement basique d'un VPN (riseup.net)

mot de passe dont la configuration dépend du VPN. Il est possible d'utiliser un VPN pour sa navigation, mais également pour ses discussions instantanées, l'utilisation de logiciels de pair à pair et pour la consultation de ses e-mails via un client.

## Points négatifs à l'utilisation d'un VPN

Les VPN ne sont pas la panacée pour être anonyme en ligne.

La trace la plus évidente est celle que vous laissez en payant. Les modalités de conservation de vos données de paiement diffèrent selon les fournisseurs de VPN, mais ces derniers peuvent souvent, d'une manière ou d'une autre, savoir qui vous êtes. Certains VPN, notamment suédois, acceptent le paiement de l'abonnement en espèces, ce qui permet d'atteindre un degré d'anonymat élevé, à condition que l'adresse e-mail utilisée pour s'enregistrer soit créée et maniée avec précaution (voir le chapitre 6). C'est aussi pour cette raison qu'il faut s'assurer que le VPN ne puisse pas faire le lien entre un compte client et son activité, même si on le lui demande.

Certains VPN sont fournis avec des logiciels qui simplifient la configuration et la mise en place. Certains nécessitent de mettre la main dans le cambouis et d'opérer les réglages directement dans les paramètres de vos logiciels (ou dans les paramètres réseau de votre machine). Cela ouvre la porte à des erreurs de configuration, et donc à de potentielles brèches dans l'anonymat de la connexion.

Il faut toujours s'assurer du bon fonctionnement de son VPN. Certains étant moins fiables que d'autres, la connexion peut parfois être interrompue.

Dans certains pays, notamment la Chine, les autorités sont capables de compliquer la tâche des VPN en détectant l'utilisation de leurs services et en bloquant le trafic[174].

Enfin, le point le plus crucial concerne la conservation des données de connexion, ou logs. Votre VPN reçoit votre connexion, il sait donc quelle est votre adresse IP, quelles sont vos habitudes de navigation… Toutes ces informations peuvent être retrouvées et éventuellement communiquées à des tiers. Dans une optique de protection de la vie privée et de l'anonymat, il convient de choisir un fournisseur de VPN qui ne conserve aucune trace de votre activité. En Europe, il n'y est légalement pas obligé, contrairement aux hébergeurs ou aux fournisseurs d'accès à Internet.

### Confiance Comment être sûr de son VPN ?

**Beaucoup de fournisseurs de VPN vous l'assurent : ils ne gardent pas de traces de votre connexion (*no log*). Comment être sûr qu'ils disent la vérité ? Ce n'est pas possible, tout est une histoire de confiance. Ces entreprises, qui basent leur activité sur le respect de la vie privée de leurs utilisateurs, ont tout de même un intérêt économique à protéger celle-ci au maximum. Dans tous les cas, il faut toujours utiliser un VPN qui inspire confiance, ou adapter son usage en conséquence.**

## Comment configure-t-on son VPN ?

En fonction du protocole utilisé et du fournisseur de VPN choisi, plusieurs scénarios peuvent s'offrir à vous.

Si un logiciel est fourni avec l'abonnement au VPN, il vous faudra sans doute l'utiliser ou vous référer aux pages d'aide du fournisseur. Si votre VPN utilise le protocole PPTP (plus d'informations sur ce protocole un peu plus loin), il est possible de paramétrer votre connexion sans logiciel particulier, directement sur votre machine (avec les informations communiquées par votre fournisseur), pour que toute votre activité réseau (e-mail, navigation, chat, P2P…) passe par votre VPN.

PRATIQUE **De nombreux guides pour tous les protocoles**

**De nombreux guides sont disponibles sur Internet pour tous les protocoles et sont utiles en cas de difficulté. Ceux du site du VPN Anonine sont très complets :**

> anonine.com/en/guides

Pour Windows (XP, Vista, 7 ou 8), Mac et Linux, il suffit de rentrer le nom du VPN, son serveur (l'adresse exacte doit vous être fournie), votre nom d'utilisateur et votre mot de passe. La figure 7-4 illustre à quoi ressemble la configuration d'un VPN en PPTP sur un iPhone.

Si votre VPN utilise OpenVPN, c'est un petit peu plus compliqué (il n'est en outre pas compatible avec tous les systèmes d'exploitation pour mobiles). Il vous faudra installer sur votre machine un logiciel tiers (sous Linux/Ubuntu, ce sera apt://network-manager-openvpn, sous Windows on pourra par exemple choisir le logiciel Viscosity). Une fois ce logiciel tiers lancé, la méthode est ensuite similaire (serveur, nom d'utilisateur, mot de passe). Votre fournisseur pourra éventuellement vous procurer un certain nombre de fichiers afin de faciliter le paramétrage de votre connexion.


Fig. 7–4 > Écran de paramétrage d'un VPN en PPTP sur un iPhone

## Pratique Quelques ressources

Plusieurs méthodes et tutoriels existent pour configurer un VPN utilisant OpenVPN. On pourra en citer quelques-uns :

- **Windows :** ipredator.se/guide/openvpn/windows/viscosity
  anonine.com/en/guides/openvpn-windows-xp
- **Ubuntu :** ipredator.se/guide/openvpn/ubuntu/gnome
- **Mac OS X :** ipredator.se/guide/openvpn/macosx/viscosity

Attention, ces méthodes, publiées par des fournisseurs de VPN, s'adressent surtout à leurs propres utilisateurs. Selon votre fournisseur, la méthode variera légèrement. Presque tous les fournisseurs proposent en tout cas des tutoriels et des explications assez claires.

## Comment choisir son VPN ?

Chaque jour, des fournisseurs de VPN apparaissent et disparaissent. N'en retenir qu'un rendrait le conseil très périssable. De plus, il y a énormément de fournisseurs de VPN, dans tous les pays. En termes de sécurité, certains paraissent très fiables… jusqu'au jour où ils font une entorse à la sacro-sainte protection de la vie privée de leurs clients. Il y a autant d'usages de VPN que d'utilisateurs. Même si l'objectif de cet ouvrage est de vous donner des clefs pour protéger votre anonymat, vous n'aurez peut-être pas les mêmes critères en matière de protection et de sécurité que l'auteur de ces lignes, ni même forcément le même usage. C'est pourquoi nous préférons ne pas vous recommander l'utilisation d'un VPN en particulier.

Notez que le site spécialisé Torrentfreak réalise à intervalles réguliers un questionnaire axé sur la protection de l'anonymat à de nombreux fournisseurs de VPN. La dernière livraison de ce baromètre fort utile est accessible ici :

> https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/

PROS **Attention aux amateurs**

**Un temps réservé aux professionnels désireux de travailler à distance en toute sécurité, le secteur des VPN a été investi par de nombreuses entreprises, à la faveur des lois sécuritaires sur le réseau qui ont fleuri aux États-Unis et en Europe. Attention aux arnaques, nombreuses sur ce marché un peu complexe.**

Le mot-clef dans l'utilisation d'un VPN est la confiance. Vous confiez en effet à un VPN une grande responsabilité : celle de gérer une partie de votre identité en ligne. C'est donc un choix informé que vous devez prendre par vous-même.

On peut lister une série de critères à prendre en compte pour faire le meilleur choix possible, en fonction des risques que vous estimez courir et de vos besoins.

**Le siège social du fournisseur de VPN**, et surtout la législation du pays dans lequel ce dernier est situé, ont une importance sur les données que le fournisseur pourra transmettre aux autorités et sur les modalités juridiques de cette transmission. Aux États-Unis, les conditions sont plus souples qu'en Suède, pays réputé pour la robustesse de ses lois protégeant la liberté d'expression. Pour plus de sécurité, on choisira un VPN qui n'est pas localisé dans le même pays que le sien.

Si la connexion entre votre ordinateur et votre VPN est chiffrée, ce n'est pas forcément le cas de la connexion entre le site visité et le VPN. Cela peut faire apparaître le contenu de votre connexion ! C'est pourquoi en complément d'un VPN, il faut utiliser une connexion en HTTPS (voir le chapitre 4).

**La localisation des serveurs du VPN est importante** : si votre VPN utilise un serveur de sortie, c'est-à-dire un serveur par lequel sort votre connexion, situé aux États-Unis, il sera soumis aux lois des États-Unis.

DISCRÉTION **Votre fournisseur d'accès à Internet sait que vous utilisez un VPN**

Si votre FAI ne voit pas ce que vous faites lorsque vous êtes connecté à un VPN, il peut cependant voir que vous en utilisez un. Cela peut être problématique dans certains pays et dans certaines situations.

À cette problématique de sécurité s'ajoute un deuxième aspect : l'utilisation que vous voulez faire de votre VPN. Si vous voulez regarder des émissions de télévision uniquement accessibles depuis les États-Unis, un VPN y disposant d'un serveur de sortie peut être une option.

**Il faut privilégier un VPN qui ne garde pas les logs de connexion**, c'est-à-dire les traces (date, durée, adresse IP) laissées par toutes vos connexions passées par le serveur du VPN. Votre adresse IP arrive sur ce serveur sans être camouflée. Si le fournisseur de VPN conserve ces informations, il peut dans certains cas les divulguer à la police, ou pire, les publier et les consulter. Même avec les meilleures intentions du monde, on ne peut pas vraiment résister à un ordre de la justice ou de la police.

Heureusement, beaucoup de fournisseurs le jurent la main sur le cœur : ils ne gardent pas les logs de connexion de leurs utilisateurs, ce qui les empêche d'avoir la moindre information à donner aux autorités.

### Double Utiliser deux VPN pour plus de protection

Pour maximiser son anonymat, on peut envisager de souscrire à deux VPN : l'un que l'on utilisera pour ses activités professionnelles, l'autre pour ses activités personnelles. Cela permettra d'utiliser deux adresses IP différentes, dont aucune n'est vraiment l'adresse IP réelle.

**Il faut ensuite choisir le bon protocole.** Deux principaux protocoles de VPN s'affrontent sur le marché : PPTP et OpenVPN. Je vous invite à fureter pour découvrir leurs différences et les meilleures compatibilités selon vos besoins.

On peut tout de même résumer de la sorte : OpenVPN est libre, plus sûr, mais plus compliqué à installer, généralement plus cher et incompatible pour le moment avec certains systèmes d'exploitation pour mobiles. Les VPN utilisant PPTP (développé originellement par Windows) sont simples à installer, compatibles avec les mobiles, généralement moins chers, mais moins sûrs (notamment avec les nouvelles adresses IPv6) et incompatibles avec certains routeurs.

CHIFFREMENT **Plus de bits pour OpenVPN**

Les VPN utilisant PPTP utilisent généralement des clefs de chiffrement de 128 bits, tandis que les solutions basées sur OpenVPN proposent fréquemment des clefs de 2 048 bits.

**La compatibilité avec les logiciels** que vous souhaitez utiliser doit également guider votre choix de VPN. Il faut vérifier le cas échéant que le pair à pair (P2P) soit accessible avec le VPN choisi. Tous les protocoles sont généralement pris en charge, mais certains fournisseurs bloquent certains types d'utilisation.

**Certains VPN sont plus rapides que d'autres**. Attention, une connexion qui utilise un VPN sera de toute façon plus lente qu'une connexion classique. Ce n'est pas forcément le plus important dans une logique d'anonymat, mais ce critère mérite tout de même d'être considéré.

ASTUCE **Essai gratuit**

Les fournisseurs de VPN proposent généralement des périodes d'essai gratuit. Cela permet de juger de la vitesse et de la fiabilité d'un fournisseur avant de s'engager.

Certains fournisseurs mettent en place des limites de trafic, de quelques centaines de mégaoctets à plusieurs gigas. D'autres limitent le nombre d'ordinateurs qui peuvent être connectés en même temps au réseau.

**Les moyens de paiement, dans une optique d'anonymat, doivent être considérés avec précaution**. Si vous ne voulez pas que votre fournisseur de VPN connaisse votre identité, même de manière indirecte, évitez les cartes bancaires et autres PayPal, mais préférez les espèces ou des solutions alternatives comme Bitcoin (lorsque le fournisseur les propose, voir chapitre 9).

Il est aussi vivement conseillé, avant de s'engager auprès d'un VPN, de lire sa politique de confidentialité et de faire le tour du Web pour voir si des consommateurs heureux (ou malheureux) se sont fait entendre ou si des experts ont donné leur avis sur ces services.

PRATIQUE **Avantages annexes du VPN**

Un VPN permet de chiffrer sa connexion lorsqu'on utilise un réseau sans fil public, ce qui est particulièrement utile dans les endroits publics où l'on peut éventuellement surveiller votre connexion (universités, bibliothèques, aéroports, etc.).

VPN **Exemples et références**

On pourra quand même donner une mention honorable en termes de protection de l'anonymat à quelques fournisseurs de VPN, dont Mullvad, Anonine ou Ipredator (tous basés en Suède).
On pourra également envisager toonux.net/vpn (lancé par Bluetouff, figure reconnue dans le milieu du hacking français), PRQ.se, privatvpn.se, privateinternetaccess.com, torguard.com, hidemynet.com ou vpntunnel.com.
Sur Internet, les listes et les comparatifs de VPN sont légion. En voici quelques-uns :

> en.cship.org/wiki/VPN
> vpn-compare.org
> korben.info/choisir-son-vpn.html
> lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs
> free.korben.info/index.php/VPN
> torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007
> torrentfreak.com/tag/vpn

# Tor, la solution la plus aboutie

Tor est sans doute la plus connue des technologies permettant l'anonymat, sans doute parce qu'elle est aujourd'hui la plus sûre.

Tor a été créée sous l'impulsion du gouvernement américain, qui cherchait à établir un réseau parfaitement anonyme. Le réseau est aujourd'hui maintenu principalement par des bénévoles, même s'il reçoit encore des fonds de la part de l'administration américaine.

De nombreux gouvernements, journalistes et activistes utilisent ce réseau.

## Comment Tor fonctionne-t-il ?

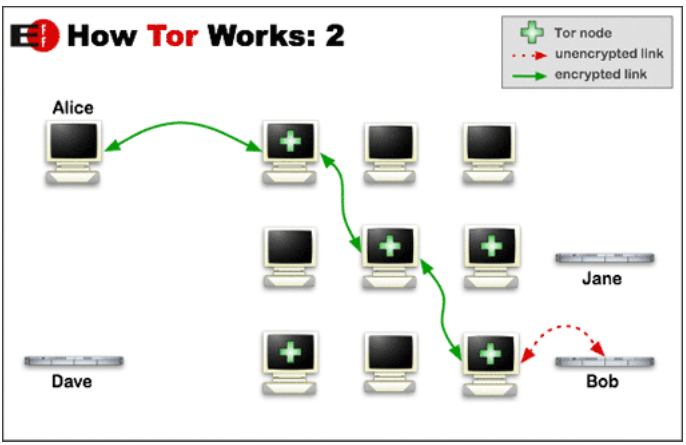



Fig. 7–5 > Le fonctionnement, à grands traits, de Tor (torproject.org et eff.org)

Dans son principe, le système de fonctionnement de Tor est simple. Au lieu d'établir la connexion directement avec le site à visiter, elle va passer par plusieurs ordinateurs différents. Lorsque le message est émis, il est empaqueté dans plusieurs couches de chiffrement (d'où le nom donné à Tor de routage en oignon), qui seront déchiffrées à chaque étape dans le réseau.

Tor a donc deux avantages majeurs : il permet de camoufler très efficacement le contenu d'une connexion, mais également son point d'origine. Il est aussi largement utilisé comme un outil anti-censure (puisqu'il permet de camoufler sa destination).

ATTENTION **Problème des extensions bavardes**

**Il est déconseillé d'utiliser des extensions dans un navigateur utilisant Tor, puisqu'elles peuvent communiquer votre véritable adresse IP. De même, les scripts présents sur les pages que vous visitez peuvent contourner Tor et révéler votre adresse IP (l'utilisation de l'extension NoScript est recommandée). Il est de toute façon conseillé d'utiliser le navigateur par défaut de Tor, qui contient toutes les protections possibles (voir plus loin).**

Étant donnée la nature de cette technologie (votre connexion empreinte des dizaines d'autres ordinateurs), il faut bien avoir à l'esprit que se connecter à Tor ralentit considérablement le débit. C'est pour cela qu'un peu plus haut dans ce chapitre, je recommandais d'utiliser Tor pour une utilisation ponctuelle ou à haut risque, et un VPN lorsque la connexion doit être plus stable et plus rapide. Cependant, cette analyse est le fruit d'un calcul coût/avantage que vous devez également faire de votre côté.

## Comment utiliser Tor ?

Tor s'utilise très simplement. Il suffit de télécharger le *Tor Browser Bundle*, sur le site torproject.org. Cliquez ensuite sur le fichier intitulé *start tor browser* et le programme se lance.

Vidalia est le programme qui va vous connecter au réseau Tor. Une fois le logo de Tor devenu vert dans Vidalia, un navigateur Firefox spécialement configuré pour protéger votre anonymat se lance.

### Astuce Une messagerie instantanée vraiment anonyme

Il est possible de paramétrer votre client de chat afin qu'il utilise Tor pour se connecter (il suffit, une fois que Vidalia est en route, de demander à votre client de se connecter avec un proxy : l'adresse du proxy doit être *localhost* et le port 9050). Si vous utilisez cette connexion pour créer un compte pseudonyme sur un serveur XMPP fiable, puis changez d'identité sur Vidalia et vous y connectez, pour ensuite discuter en activant la technologie OTR, vous vous approchez très fortement de l'anonymat total.


Fig. 7–6 > Vidalia est lancé, le logo de Tor s'affiche en vert, vous êtes connecté !

Plusieurs options sont disponibles depuis Vidalia, notamment celle qui permet de partager sa connexion. Tor étant un réseau décentralisé, n'importe qui disposant d'une connexion à Internet peut utiliser cette dernière comme relais. Il suffit de cliquer sur *Installer un relais* pour le faire. Il existe deux types de

relais : les *non exit relays*, c'est-à-dire que les utilisateurs de Tor ne feront que passer par votre connexion, et des *exit relays*, que les utilisateurs de Tor prendront pour sortir (c'est donc votre adresse IP qui apparaîtra dans leur connexion, ce qui n'est pas sans poser quelques questions juridiques).

Depuis Vidalia, il est également possible de choisir une autre identité, c'est-à-dire un autre « chemin » dans le réseau Tor, et d'adopter en conséquence une adresse IP différente. C'est idéal si vous voulez qu'un site ne détecte pas vos visites récurrentes, même si par défaut votre connexion emprunte un chemin différent toutes les dix minutes.

ATTENTION **N'ouvrez pas les documents téléchargés sur Tor**

Il faut à tout prix éviter d'ouvrir les documents éventuellement téléchargés lors de votre navigation sur Tor, ces derniers pouvant révéler votre adresse IP. Il convient de les ouvrir sur une machine déconnectée d'Internet ou sur une machine virtuelle sans connexion.

Tor a le même problème que beaucoup de technologies : son utilisation est assez facile à détecter et peut à elle seule révéler un comportement potentiellement suspect pour certaines autorités. Heureusement, il est possible de mettre en place une solution technique appelée Tor bridge, qui camoufle l'utilisation de Tor.

JAMAIS **Ne jamais utiliser Tor pour faire du pair à pair**

Tor est un réseau maintenu par des bénévoles, qui donnent un peu de leur bande passante pour que des activistes ou des internautes soucieux de leur vie privée puissent se protéger. Il n'est absolument pas prévu pour transporter de grandes quantités de données (il est déjà assez lent). Il est donc absolument absurde (et, si vous voulez mon avis, immoral) d'utiliser Tor pour télécharger en peer-to-peer. De plus, cette combinaison ne protège que très partiellement votre identité[175].

## Tor est-il vraiment sécurisé ?

Malgré l'origine gouvernementale de Tor, cette technologie peut être considérée comme complètement sûre, notamment parce qu'elle est open source. « Tor a été décortiqué pendant des années. Toutes les failles ont été trouvées et réparées. Grâce à ça, c'est mieux que le reste. C'est le seul système d'anonymat solidement audité pour les communications en temps réel », estime Chris Soghoian, un des meilleurs experts du sujet[176].

On peut imaginer qu'un gouvernement mette en place un nombre suffisamment important de nœuds de réseaux pour avoir une idée précise du contenu et de l'origine des connexions qui passent par Tor. En réalité, vu la taille déjà grande du réseau, il devrait y consacrer des ressources très importantes (qui ne passeraient pas inaperçues) et serait de toute façon en concurrence avec d'autres gouvernements.

Tor comporte des failles (notamment au niveau de ses nœuds de sortie), comme tout système de sécurité informatique ou de cryptographie. Pour le moment néanmoins, aucun utilisateur de Tor n'a jamais été identifié, malgré les efforts de la NSA[177].

## Autres réseaux anonymes

Il existe également des réseaux moins connus permettant d'être anonyme.

Citons d'abord Freenet (freenetproject.org), une sorte de réseau parallèle à Internet. Il fonctionne de manière assez similaire : lorsqu'on s'y connecte, on peut naviguer de page en page comme sur le Web classique. La particularité de ce réseau, c'est qu'il est complètement décentralisé : chaque utilisateur de Freenet stocke une partie des contenus de tout le réseau. Les contenus les plus populaires sont répliqués plusieurs fois. Toutes les informations stockées par les utilisateurs sont chiffrées, il est donc impossible de savoir ce qui est stocké. Le seul

moyen d'y accéder, c'est de passer par Freenet. Il n'est alors plus possible de savoir quel contenu est stocké sur quelle machine. Freenet, de par sa conception complètement décentralisée, est impossible à arrêter. Pour utiliser Freenet, il suffit de télécharger le logiciel du même nom sur freenet.sourceforge.net.

Partiellement payant, le logiciel JAP (ou JonDoNym) permet une navigation relativement sécurisée, notamment parce qu'il joue le rôle d'une sorte de super proxy entre l'ordinateur de l'internaute et celui du site visité. Au lieu de se connecter directement à un serveur web, les utilisateurs font un détour en se connectant de façon chiffrée via plusieurs intermédiaires. JAP a été développé par des universités allemandes et peut être utilisé via Firefox ou avec un logiciel dédié. Pour le télécharger : anonymous-proxy-servers.net/en/software.html.

Le logiciel open source Psiphon, développé par une entreprise canadienne du même nom, utilise un mélange de VPN, de SSH et de proxies pour contourner la censure. Il peut être téléchargé sur psiphon.ca.

Ultrasurf est un logiciel, non open source, de contournement et d'anonymat très largement utilisé depuis de nombreuses années[178] par plusieurs dizaines de millions de personnes, partout dans le monde et plus particulièrement en Chine.

Début 2012, le chercheur et activiste Jacob Appelbaum, proche de Wikileaks et du projet Tor, a effectué un audit très poussé du logiciel et a pointé plusieurs failles cruciales[179]. La réponse de Ultrareach, la société qui édite Ultrasurf[180] n'a pas convaincu la communauté[181]. Aujourd'hui, les deux camps s'affrontent et entre les failles corrigées, les failles encore présentes et les querelles liées au processus d'évaluation du logiciel, il est difficile d'y voir clair. Les travaux détaillés de Appelbaum sont disponibles en ligne[182].

# 8 Sécuriser son smartphone et sa tablette

*Depuis plusieurs années, les mobiles et les tablettes ont pris des places considérables dans nos vies numériques. Problème : les outils de protection des communications sont pour la plupart d'abord conçus pour les ordinateurs. Néanmoins, ce retard commence à être rattrapé.*

## Le contexte mobile

Les téléphones mobiles sont très largement utilisés, mais la technologie étant assez récente, on ne dispose pas d'autant de recul que sur Internet ; les technologies performantes sont encore balbutiantes. Il est donc très difficile de sécuriser correctement un téléphone mobile.

Le danger vient en grande partie des applications que l'on installe : soyez prudent et utilisez des applications open source lorsque c'est possible.

Gardez à l'esprit que le seul vrai moyen de rester anonyme en utilisant un téléphone portable… est de ne pas en utiliser du tout !

## Les faiblesses de votre téléphone

À chaque fois que vous passez un appel, sa date, sa durée, le numéro que vous avez composé, ainsi que votre localisation approximative sont enregistrés par votre opérateur. Ces données peuvent être requises par les autorités de police sur simple demande auprès de l'opérateur. Plus généralement, diverses informations comme le numéro IMEI ou la carte SIM, soit votre identité, sont associées à de nombreuses activités du téléphone.

### Loi Le législateur américain s'inquiète au sujet des mobiles

**De plus en plus d'hommes politiques américains s'inquiètent du nombre de données personnelles captées et utilisées par les applications mobiles[183].**

Dès que votre téléphone se connecte à Internet, les choses se compliquent encore. Votre téléphone communique en effet en permanence avec Internet, notamment parce que de nombreuses applications fonctionnent en arrière-plan. Apple et Google, dans leurs systèmes d'exploitation pour mobiles respectifs, scannent les réseaux Wi–Fi en permanence pour en dresser la carte et améliorer leurs fonctionnalités de géolocalisation. De nombreuses applications utilisent par ailleurs cette technologie souvent activée par défaut, notamment les applications pour photos ou les réseaux sociaux. On estime qu'une application Android gratuite sur quatre suit votre localisation[184] et 7 % d'entre elles ont accès à votre carnet d'adresses. Il est possible, pour tous les smartphones, de désactiver la fonction de géolocalisation.


FIG. 8–1 > L'écran de paramètrage de la géolocalisation sur un iPhone

Il faut noter que, dans le cas des téléphones Android, la géolocalisation est activée par défaut, ce qui permet à Google de dresser l'historique très précis de vos déplacements. Ces derniers sont accessibles à l'adresse google.com/locationhistory lorsque vous êtes connecté à votre compte. Il est fortement conseillé de désactiver cette option (depuis la même adresse), tant elle semble intrusive et n'apporte pas de fonctionnalité supplémentaire.

Les communications émises par les téléphones peuvent être interceptées facilement. Simplement en se trouvant à proxi-

mité, les applications que vous installez peuvent avoir accès à des données personnelles et les envoyer sur leurs propres serveurs sans vous en avertir. De plus, les données qui sont stockées sur votre téléphone, la plupart du temps en clair, sont facilement accessibles.

## Gérer les autorisations des applications

Plus largement, il est conseillé de se plonger dans les paramètres de votre téléphone pour gérer à la fois les paramètres de localisation et les autorisations de vos applications, c'est-à-dire à quelles données (données, calendriers...) elles ont accès.

On citera une application pour Android qui peut être téléchargée sur forum.xda-developers.com/showthread.php?t=1357056. Open source, cette application nécessite cependant de « rooter » son téléphone. L'application Droidwall fonctionne de manière assez similaire (code.google.com/p/droidwall).

### Surprise Sur l'iPhone, quelques options cachées à désactiver

**Deux petites fonctionnalités qui vous tracent sont activées par défaut sur les iPhone et sont très faciles à désactiver. La première se nomme *Lieux fréquents*. Il s'agit d'une carte des lieux dans lesquels vous vous rendez le plus ! Elle est accessible (et désactivable) dans *Paramètres* > *Confidentialité* > *Service de localisation* > *Services système* > *Lieux fréquents*. De même, dans *Paramètres* > *Confidentialité* > *Publicité*, il est possible de paramétrer son iPhone pour que le suivi publicitaire soit limité.**

Si vous utilisez un téléphone ou une tablette Android, il est très facile d'en chiffrer intégralement le contenu, le rendant illisible par quiconque ne disposant pas du code[185]. Ce paramétrage présente toutefois deux inconvénients : cela rend le terminal plus lent et, pour mettre fin au chiffrement, il faut le

réinitialiser à ses valeurs d'usine. Cette fonctionnalité est accessible depuis *Paramètres* > *Sécurité*.

## Passer des appels chiffrés

Les solutions pour téléphoner de manière sécurisée ne sont pas très nombreuses.

On pourra citer https://ostel.co, un protocole ouvert sur lequel il est nécessaire de créer un compte, avant de se procurer pour sa tablette ou son mobile l'application pour le mettre en pratique. Une liste est disponible sur https://ostel.co/about.

La start-up WhisperSystems propose également RedPhone, une application destinée à passer des appels. Disponible uniquement sur Android, vous pouvez la télécharger sur https://play.google.com/store/apps/details?id=org.thoughtcrime.redphoneg. Le code source de cette application est ouvert. L'entreprise a également réalisé un équivalent pour iPhone, Signal, dont le code est ouvert. Cette application peut être téléchargée à cette adresse : https://itunes.apple.com/app/id874139669.

Discretio (discretio.com) propose également une application en version d'essai (attention aux bogues !), open source elle aussi.

## Sécuriser ses messages texte

Plus spécifiquement, quelques solutions peuvent être envisagées pour chiffrer les SMS envoyés depuis un mobile.

On rappellera d'abord que les iMessages (les messages spécifiques à l'iPhone d'Apple) ainsi que FaceTime (son système de VoIP) sont chiffrés. Cela offre une première couche de sécurité, même si Apple demeure capable de les déchiffrer, notamment sur ordre du gouvernement (Apple fait partie du programme Prism).

Il est tout de même conseillé, pour un niveau de sécurité optimal, d'opter pour une autre solution.

Plusieurs applications disposent de versions pour Android et iPhone. Aucune n'est parfaitement satisfaisante en termes de sécurité (open source, technologiquement avancée, située dans un pays favorable, auditée en profondeur), mais certaines méritent le détour pour quelques usages, notamment parce qu'il peut s'agir de bonnes alternatives aux applications développées par les géants du Web comme Whatsapp (rachetée par Facebook), Facebook Messenger ou Google Hangouts. On peut par exemple citer Hoccer (hoccer.com), une application développée en Allemagne par un ancien du très célèbre Chaos Computer Club (réputé pour ses combats pour la vie privée en ligne), Seecrypt (seecrypt.com) ou Telegram (telegram.org), bien que des experts aient repéré plusieurs failles dans cette application, popularisée après le rachat de Whatsapp.

E-MAILS **PGP sur son mobile**

**Si vous souhaitez utiliser PGP pour chiffrer vos e-mails depuis votre mobile (voir chapitre 6), plusieurs applications, sous Android uniquement, peuvent vous être utiles :**

- **Openkeychain (**openkeychain.org**)**
- **K-9 Mail (**https://play.google.com/store/apps/details?id=com.fsck.k9**)**
- **APG (**http://www.thialfihar.org/projects/apg/**).**

Pour les utilisateurs d'Android, on recommandera TextSecure, l'application open source développée par WhisperSystems, assez reconnue dans le milieu de la sécurité. Elle est téléchargeable sur whispersystems.org.

Cryptocat (voir chapitre 7) dispose d'une version iOS (la version pour Android est en cours de développement).

D'autres applications prometteuses sont également en développement, par exemple Hemlis (heml.is) ou FoilChat (foilchat.com).

## Solutions tout-en-un : tout faire avec un seul outil

De nombreuses entreprises ou organisations s'engouffrent dans la demande de vie privée des internautes et des possesseurs de smartphones. En voici quelques-unes.

Wickr (mywickr.com) propose des solutions de chiffrement pour l'envoi de photos, de textes, d'audio et de vidéos. Leur technologie n'est pas open source (à utiliser avec encore plus de précaution), mais leur politique de vie privée est intéressante et la technologie utilisée est puissante. Leurs solutions sont disponibles sur iOS (iPhone), ce qui est rare.

Le *Guardian Project*, très reconnu en sécurité informatique et défense des libertés numériques, propose sur son site (guardianproject.info/apps) une foule d'applications orientées anonymat et sécurité, notamment pour la messagerie instantanée, les SMS ou les appels.

Silent Circle (silentcircle.com), dont nous avons déjà parlé au chapitre 6, propose une solution pour chiffrer ses SMS et ses appels.

## Naviguer de manière sécurisée

On conseillera aux possesseurs d'iPhone d'abandonner Safari pour leur navigation, et aux possesseurs d'Android d'oublier Google Chrome. De manière générale, il vaut mieux éviter le navigateur par défaut de votre téléphone. Mozilla a lancé sur Android la version mobile de son navigateur Firefox (mozilla.org/fr/mobile), que nous vous recommandons d'utiliser.

Pour les utilisateurs d'iPhone et d'iPad, le choix est plus compliqué : deux navigateurs ont bonne réputation, Dolphin (dolphin-browser.com) et Atomic Web Browser (atomicwebbrowser.com).

Il est par ailleurs possible d'utiliser Tor (voir le chapitre 7) depuis son smartphone Android. L'application est disponible sur https://guardianproject.info/apps/orweb/. Un équivalent existe pour iPhone : Onion Browser (mike.tig.as/onionbrowser).

## Chats

Il est envisageable d'utiliser le protocole de discussions instantanées XMPP (voir chapitre 6) depuis un téléphone mobile. On recommandera tout particulièrement ChatSecure (ex-GibberBot, chatsecure.org), ainsi que Xabber (xabber.org), uniquement sur Android.

## Utiliser un VPN avec son téléphone

Il est possible d'utiliser un VPN (voir chapitre 7) avec la plupart des téléphones mobiles récents, ce qui résout une petite partie du problème lié aux connexions permanentes de votre téléphone à Internet (il est également possible de désactiver la connexion Internet de votre téléphone lorsque vous ne vous en servez pas, évidemment).

Les fournisseurs de VPN mettent généralement à la disposition de leurs clients des tutoriels pour installer leurs services sur mobile et tablette.

On notera, pour les utilisateurs d'Android, l'application du Guardian Project, Orbot (https://guardianproject.info/apps/orbot/), qui va faire transiter à travers Tor le trafic lié à de nombreuses applications sur votre téléphone. Cela veut dire que votre navigation, votre utilisation de Twitter ou vos discussions instantanées seront plus anonymes. C'est une bonne solution tout-en-un.

# Remplacer son téléphone ou son système d'exploitation

La sécurité des applications et des programmes présentés dans ce chapitre dépend aussi de la sécurité du système d'exploitation, le logiciel qui fait fonctionner votre téléphone. Or, on sait bien que Google comme Apple collaborent de près avec les agences de renseignement des États-Unis. De plus, iOS, le système d'exploitation développé par Apple, est complètement opaque et fermé : on ne sait pas ce qui s'y passe ni quelles sont les données collectées ou les failles exploitables.

Une solution radicale pour sécuriser ses communications et sortir de la dépendance de Google ou d'Apple peut donc consister à changer de système d'exploitation.

Pour le moment, peu de possibilités s'offrent à vous : les utilisateurs d'Android peuvent installer CyanogenMod (http://www.cyanogenmod.org/), une version modifiée d'Android, de plus en plus stable, efficace et facile d'installation, ou Firefox OS, le système d'exploitation libre développé par Mozilla, la fondation derrière le navigateur Firefox.

### Aller plus loin « Rooter » son téléphone

**Les fabricants de téléphones mettent souvent en place des verrous qui empêchent de faire et d'installer ce que l'on veut. Il est possible de supprimer ces verrous : c'est ce qu'on appelle « rooter » ou « jailbreaker » son téléphone. Le problème, c'est que cela consiste à remplacer le logiciel fonctionnant sur son téléphone par un autre, sans savoir précisément ce que fait ce dernier (à moins qu'il soit open source). Sur les iPhone d'Apple, jailbreaker son téléphone consiste à le transformer en une sorte de mini-serveur, ce qui accroît en fait sa vulnérabilité. Si des assaillants arrivent à y pénétrer (même à distance), ce sont toutes vos données qui risquent d'être compromises. Cette solution doit donc être considérée avec précaution.**

Enfin, ceux qui peuvent se permettre d'investir pour se protéger peuvent envisager l'achat du Blackphone (blackphone.ch), un téléphone développé par l'entreprise Silent Circle et une entreprise suisse, qui prétend offrir toute une panoplie de fonctionnalités permettant la protection de la vie privée, le tout sur un système d'exploitation garanti sans surveillance.

# 7 Se protéger mieux et aller plus loin

*Le champ de la sécurité informatique au service de l'anonymat est extrêmement vaste. Voici quelques outils, techniques et réflexes complémentaires.*

## Protéger son mot de passe

Le mot de passe est un des éléments les plus cruciaux et les plus utilisés dans le champ de la sécurité informatique. C'est aussi, souvent, le seul rempart entre vos données personnelles, votre identité et le monde extérieur. Il est donc absolument fondamental de savoir comment créer un bon mot de passe. Au-delà de l'anonymat, qu'il protège parce qu'il empêche de croiser des comptes, des données, des identités en morcelant, avoir un bon mot de passe protège contre bien des mauvaises surprises.

### Vulnérabilité inhérente

Le mot de passe est, à peu de chose près, la seule protection accessible au grand public en matière de

sécurité informatique. Le problème, c'est que le niveau de sécurité qu'il procure est assez faible.

Les innovations techniques sont innombrables et leur vulnérabilité sans cesse rappelée. Aujourd'hui, les articles dans la presse se multiplient et prouvent que les mots de passe n'ont jamais été aussi faibles[186]. Plusieurs raisons à cela, et notamment les nombreuses fuites de mots de passe, permettent aux pirates de connaître très précisément la manière dont les utilisateurs les créent et les utilisent. Ces gigantesques listes sont incorporées aux logiciels utilisés par les pirates pour davantage d'efficacité. Les progrès technologiques jouent aussi une part importante : un nouveau processeur capable de briser des mots de passe Windows standard en moins de six heures a été récemment mis sur le marché[187].

ASTUCE **Tester son mot de passe**

**Vous vous demandez si votre mot de passe est résistant ? De nombreux sites proposent d'en évaluer la sécurité. Même s'il faut avoir suffisamment confiance pour lui confier son mot de passe, on testera par exemple** myshadow.org/sites/myshadow.org/password-strength2.

## Les commandements du bon mot de passe

Pour s'assurer un mot de passe résistant, il faut lui appliquer quelques règles. Les spécialistes n'hésitent pas à qualifier ces règles de véritable « hygiène ». Voici quelques principes :

- Il faut privilégier la longueur à la complexité. Vous entendrez souvent qu'il faut que votre mot de passe comporte des chiffres, des caractères spéciaux et autres signes cabalistiques. C'est vrai, mais c'est au détriment de la facilité de mémorisation. De plus, un mot de passe avec un faible nombre de caractères, même rempli de signes obscurs, est très facile à casser pour une machine. Il faut donc trouver un juste milieu. De fait, `motdepasse1400contenantunerepliquedefilm1990`

est plus sûr que `[y9Çu%*||,}`. Les mots de passe les plus sûrs sont des phrases de passe (voir le chapitre 6). On peut ainsi utiliser des phrases de chansons, de livres, des citations, des langues différentes (si ces derniers ne sont pas connus).

- Un bon moyen de complexifier ses mots de passe tout en les rendant facilement mémorisables consiste à établir une routine de mot de passe. Par exemple, tous les mots de passe peuvent répondre au schéma : nom d'animal + quatre chiffres toujours les mêmes + mot lié au site sur lequel vous vous inscrivez. Sur un forum de discussion sur Star Wars, ce pourrait être `serval1977etoilenoire`. Vous avez à la fois un mot de passe relativement solide et facilement mémorisable.
- Ne pas le noter, sur quelque support que ce soit. Évitez le grand classique du post-it derrière le clavier ou la photo du bureau.
- Il ne faut évidemment le communiquer à personne. Et surtout pas sur Internet.
- Il ne doit pas comporter de mentions personnelles. Oubliez le nom de votre mari, de votre chien, ou votre chanson préférée. Les pirates ont recours à l'ingénierie sociale (fracturer les systèmes d'information sans utiliser une seule ligne de code) et ce genre d'information n'est jamais difficile à trouver (vous avez bien dû écrire le nom de votre chien sur un réseau social). Il est même préférable de ne pas utiliser de véritable mot existant dans le dictionnaire.
- Choisissez un mot de passe unique. Autrement dit : il vous faut un mot de passe différent pour chaque service utilisé ! C'est difficile, mais souvent le point le plus vulnérable. Si un intrus arrive par exemple à trouver votre mot de passe sur une plate-forme grâce à une faille de sécurité et si vous utilisez ce dernier partout, c'est très dangereux. Et si certains sites sont convenablement protégés contre des fuites de mots de passe d'utilisateurs (banques, grands réseaux sociaux), d'autres le sont moins (start-ups par exemple). On

estime que le principal danger d'une fuite de mots de passe n'est pas l'accès à la plate-forme piratée elle-même, mais à toutes les autres sur lesquelles les victimes emploient le même nom d'utilisateur et le même mot de passe !

- Certains mots de passe sont plus précieux que d'autres : celui qui vous donne accès à votre compte sur un obscur forum de discussion est moins sensible que celui qui ouvre votre boîte e-mail (dans laquelle arrivent tous les messages lorsque vous demandez une réinitialisation des mots de passe utilisés sur les autres services).
- Il faut en changer régulièrement (tous les 90 jours est un bon rythme pour les mots de passe les plus sensibles, un an pour les plus inoffensifs).

**DÉBAT N'utiliser qu'un seul mot de passe pour tous ses services ?**

Pour la plupart des utilisateurs, un seul mot de passe les protège en dernier recours du pire : celui de leur boîte e-mail, puisqu'il faut avoir accès à la boîte e-mail pour réinitialiser un mot de passe d'un compte ouvert sur un service ou un site. Si un attaquant dispose du mot de passe de la boîte e-mail, il peut ensuite réinitialiser un par un les mots de passe de tous les comptes du véritable propriétaire. Partant de ce principe, on peut imaginer n'utiliser qu'un unique mot de passe, celui de sa boîte e-mail. À chaque fois que l'on veut se connecter sur un service ou un site, on demande la réinitialisation du mot de passe, qui est envoyé, renouvelé à chaque fois, dans sa boîte e-mail. Même si cela a le mérite de limiter le nombre de mots de passe à retenir, encore faut-il que le service qui réinitialise le mot de passe en crée un suffisamment sécurisé (une alternative consiste à en générer un très complexe dont on ne fait même pas l'effort de se souvenir). De plus, cela rend la connexion à un site ou un service beaucoup plus longue.

## Des logiciels pour stocker vos mots de passe

Certains logiciels ont été développés afin de faciliter la mémorisation des mots de passe et d'en sécuriser l'utilisation.

Passpack (passpack.com) est un outil principalement destiné à ceux qui ont besoin de partager des mots de passe (avec des collè-

gues par exemple), mais qui peut être utile pour les internautes individuels. Ce service stocke de manière sécurisée (chiffrage et transmission via SSL) des mots de passe qui sont accessibles via une phrase de passe unique très complexe.

Dashlane est un logiciel (non libre) qui s'installe sur votre ordinateur et stocke les mots de passe de manière chiffrée (y compris votre adresse ou vos coordonnées de cartes bancaires). Les données ne circulent pas sur Internet.

Keepass est également un logiciel, libre et open source, qui permet de gérer ses mots de passe en un unique endroit.

## Systèmes d'exploitation orientés sécurité

Plusieurs systèmes d'exploitation ont été spécialement développés ou adaptés dans une optique de sécurité et d'anonymat.

On citera notamment le projet très abouti Tails (tails.boum.org). Le principe est simple : contenu sur une clef USB insérée dans un ordinateur éteint, il forcera la machine à démarrer sur le système d'exploitation que la clef contient.

À l'intérieur, tout l'attirail du parfait anonyme : toutes les communications sortantes passent par Tor, des logiciels de chiffrement de fichier sont installés et tous les logiciels (e-mails, discussion instantanée) sont paramétrés pour un maximum d'anonymat. Après avoir fini d'utiliser l'ordinateur, toute trace de votre passage est supprimée. C'est le système idéal pour utiliser des ordinateurs publics. La preuve de sa robustesse ? Edward Snowden l'a utilisé pour échapper à son ancien employeur, la NSA[188].

De nombreuses autres alternatives, comme Knoppix ou AnonymOS, sont listées sur free.korben.info/index.php/OS_Sécurisés_(Systèmes_d'exploitations). Tails reste la solution la plus facile à prendre en main.

Pour les utilisateurs experts, on conseillera l'usage de machines virtuelles. L'intérêt est de compartimenter au maximum ses activités en ligne (réseaux sociaux, navigation classique, navigation sensible) et d'allouer à chacune d'entre elles un système d'exploitation étanche.

**Truc Pour les webmasters**

**Vous gérez un site Internet ? Il est possible de prendre quelques mesures pour limiter les atteintes à la vie privée de vos utilisateurs : s'assurer que votre site est accessible en HTTPS (demandez à votre hébergeur), sécuriser les données que vous donnent les utilisateurs (mots de passe notamment), éviter l'utilisation de Google Analytics (lui privilégier son alternative libre Piwik), des boutons de réseaux sociaux et de la publicité (voir le chapitre 5) et prévoir une version simplifiée et sans scripts pour une navigation optimisée sur Tor. De nombreux autres conseils sont présents dans cette présentation :**

> eff.org/sites/default/files/filenode/hope_privacy_tricks.pdf

# Les fournisseurs d'accès à Internet (FAI)

On n'est pas du tout anonyme quand on souscrit un abonnement Internet auprès d'un FAI : on donne son nom, une preuve de domicile, une copie de pièce d'identité, une adresse, un moyen de paiement. Or, c'est ensuite grâce à leurs services, en faisant appel à leur technologie et à leurs serveurs que l'on va naviguer sur Internet.

Les FAI sont devenus les acteurs principaux de l'identification des internautes et peuvent (voire doivent) faire le lien entre une adresse IP et une identité. Ils sont de plus en plus impliqués dans la lutte contre la contrefaçon, laquelle requiert une identification des internautes contrevenants. C'est au FAI que revient en dernier ressort la responsabilité de l'identification de l'internaute. Il est devenu « l'incontournable identificateur des internautes sur la

Toile », réduisant, sous la pression des juges et du législateur, « les possibilités d'anonymat des internautes[189] ».

Les solutions évoquées dans le chapitre 7 peuvent être d'un grand secours pour éviter ce type de surveillance. On notera, depuis quelques années, l'apparition de FAI associatifs (cela dit, le plus ancien FAI de France, FDN, est associatif). S'ils sont souvent plus respectueux de votre vie privée (tout en devant se conformer à la loi), il faudra cependant mettre la main à la pâte pour l'installation et le fonctionnement. Plus d'informations sur ffdn.org.

### Loi L'anonymisation des données de connexion

**L'article L-34 du Code des postes et des communications électroniques impose aux fournisseurs « d'accès à des services de communication au public en ligne » de rendre anonymes les données de connexion au bout d'un an (sauf pour le fonctionnement technique et l'identification judiciaire).**

## Payer en restant anonyme

Pendant longtemps, payer a condamné l'internaute à laisser une trace. Toutefois, une solution alternative a émergé : le bitcoin.

Le bitcoin est une monnaie cryptographique décentralisée. Chacun peut lancer un programme qui « mine », c'est-à-dire crée des bitcoins. Cela nécessite, pour être efficace, une grosse puissance de calcul et le montant total qui peut être « miné » est évidemment limité.

Bitcoin, à la différence des monnaies traditionnelles, ne passe pas par une banque centrale. Chaque transaction est enregistrée et cryptographiquement signée de manière à assurer les transactions (et notamment qu'on ne puisse pas dépenser deux fois le même bitcoin). Tout est, en théorie, anonyme, puisqu'il suffit de créer un porte-monnaie bitcoin pour rece-

voir et envoyer des fonds dans cette monnaie. À défaut de pouvoir « miner » des bitcoins, il est possible de convertir de la monnaie traditionnelle.

De plus en plus de services acceptent cette monnaie. À l'heure d'écrire ces lignes, un bitcoin vaut un peu moins de 500 euros.

> https://bitcoin.org/fr/

# Aider ceux qui veulent être anonymes

De nombreuses technologies ont besoin du concours des internautes pour permettre à d'autres de se protéger.

## Aider les utilisateurs de Tor

Si vous utilisez Tor, il est possible de donner un peu de votre bande passante en transformant votre ordinateur et votre connexion à Internet en un « nœud » du réseau. Ainsi, votre ordinateur devient un des innombrables relais nécessaires à l'anonymisation des connexions des internautes utilisant Tor. Les connexions chiffrées d'internautes vont désormais transiter de manière invisible sur votre ordinateur. Cette procédure est évidemment sans danger et modifie peu votre vitesse de connexion. Surtout, plus il y a d'ordinateurs dans le réseau, plus Tor est fiable et rapide.

Cela peut se faire très facilement depuis les paramètres de Vidalia, le programme qui permet de se connecter au réseau Tor (voir le chapitre 7).

Plus technique : il est possible de configurer votre connexion Internet et votre ordinateur pour qu'ils deviennent un nœud de sortie. Cela demande davantage de ressources, d'organisation et d'implication de la part de celui qui fait ce choix. Si les

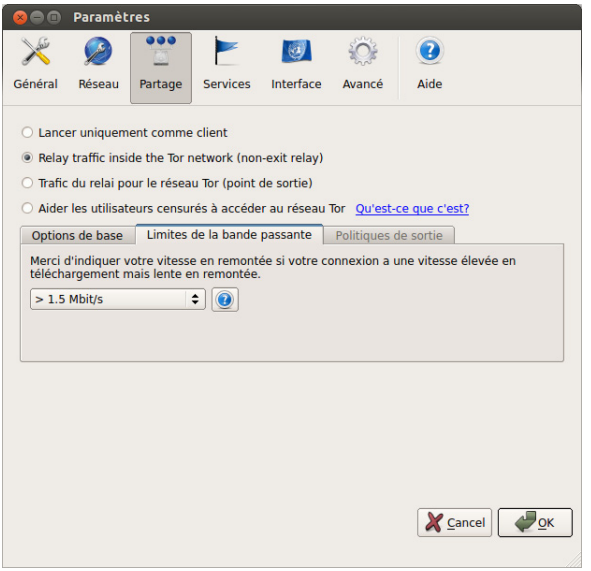



FIG. 9–1 > Le panneau de contrôle de Vidalia

données sont chiffrées lorsqu'elles circulent à l'intérieur du réseau, elles ne le sont plus quand elles sortent via un nœud de sortie. En effet, ce sont les nœuds de sortie qui vont « lire » le Web à la place d'un utilisateur dans un pays censuré. Il faut donc être capable de sécuriser ce nœud de communication vital pour permettre aux utilisateurs à l'autre bout du réseau de sortir en toute sécurité. L'autre problème, c'est que l'adresse IP du nœud de sortie sera associée à toutes les activités, éventuellement sujettes à des plaintes (téléchargement illégal, spam). En France, par exemple, ce serait un motif de condamnation pour non-sécurisation de sa ligne, en vertu de la loi Hadopi. Certains utilisateurs ont eu quelques ennuis en faisant de leur connexion personnelle un nœud sortant[190].

On recommandera donc à ceux que l'initiative intéresse d'envisager de paramétrer leur serveur comme nœud de sortie

et de se rendre sur le site de Tor, où de précieux (mais techniques) conseils les attendent.

> blog.torproject.org/blog/tips-running-exit-node-minimal-harassment

Enfin, il est possible d'aider les utilisateurs de Tor qui verraient leur accès bloqué (car il est assez facile pour des autorités d'un pays peu démocratique de savoir que tel internaute utilise Tor) en mettant en place des ponts (Torbridges). Ces ponts sont des sortes de nœuds cachés : il n'existe pas de liste exhaustive de ces derniers. Ils servent de point d'accès au réseau Tor.

> torproject.org/bridges

### Donner de la bande passante… ou de l'argent !

Si vous disposez d'un serveur, vous pouvez y installer un logiciel de serveur de proxy comme (jmarshall.com/tools/cgiproxy). Ensuite, il sera possible de se servir de votre machine comme d'un proxy web traditionnel. Vous pouvez également installer le logiciel Circumventor (peacefire.org/circumventor).

Enfin, de nombreuses organisations, qui se battent pour la liberté des internautes et pour la protection de leurs vies privées, acceptent des donations ! Le projet Tor, Freenet, l'Electronic Frontier Foundation, RiseUp… presque tous les outils que vous serez amenés à utiliser comportent un petit bouton pour donner rapidement quelques euros. Pensez-y !

## S'informer et aller plus loin

Internet regorge de documentations et de ressources variées si vous voulez approfondir ces thématiques et aller plus loin pour protéger votre identité en ligne. De plus, les technologies

avançant très rapidement, votre protection dépend très fortement de votre niveau d'information.

CONTACT **Joindre l'auteur**

**L'auteur de ces lignes peut également être contacté pour questions, remarques ou suggestions. L'identifiant de sa clef PGP devrait vous suffire : 0xC3170622. Vous avez un trou de mémoire ? Consultez la partie « Cryptographie et chiffrement » du chapitre 6.**

Les « cryptoparties » : ces rassemblements, à mi-chemin entre la réunion d'experts, l'atelier et le cours pour les débutants, visent à sensibiliser les internautes à la protection de leur vie privée sur Internet et permettent de se faire expliquer PGP, HTTPS et autres SSL par des geeks chevronnés. Regardez s'il y en a près de chez vous : cryptoparty.org !

Dans le cadre des cryptoparties, des activistes ont collaboré pour mettre sur pied le manuel des cryptoparties (cryptoparty.org/wiki/CryptoPartyHandbook), une lecture dense, mais extrêmement complète. Sa rédaction étant participative, il faut tout de même prendre quelques précautions.

Le livre (gratuit) *Comment contourner la censure sur Internet*, disponible en ligne (howtobypassinternetcensorship.org), est une mine d'informations sur la censure, son contournement et la protection de l'identité sur Internet.

Dans la même veine, le site Security in-a-box est un incontournable (securityinabox.org/fr).

Le blogueur Korben héberge un wiki (site participatif) titanesque, bourré de conseils (parfois contestables mais toujours intéressants) : free.korben.info/index.php/Accueil.

Les listes de diffusion orientées liberté numérique et sécurité informatique sont parfois riches de ressources (et de discussions enflammées). La plus régulière et la plus riche (qui voit intervenir des experts mondialement reconnus) est sans doute celle

de la très prestigieuse université de Stanford, « Liberation Tech » : mailman.stanford.edu/mailman/listinfo/liberationtech.

Le collectif Tactical Tech a mis sur pied un site passionnant sur les traces que l'on laisse sur Internet : myshadow.org. Le site de l'ONG est également très recommandable : tacticaltech.org.

L'ONG américaine Electronic Frontier Foundation a rédigé un guide très complet sur l'autodéfense numérique : ssd.eff.org.

L'ONG Frontline Defenders a quant à elle publié un e-book au format PDF extrêmement dense et fourni, destiné à la protection numérique et à la vie privée des activistes en faveur des droits humains : frontlinedefenders.org/esecman.

L'ONG française Reporters Sans Frontières n'est pas en reste, puisqu'elle a publié en 2009 un *Guide pratique du blogueur et du cyberdissident* : fr.rsf.org/guide-pratique-du-blogueur-et-du-12-03-2009,14997.html

Le wiki de la censure sur Internet (en.cship.org/wiki/Main_Page) mérite lui aussi le détour.

Les symposiums PET (*Privacy Enhancing Technologies*), qui se tiennent chaque année, donnent toujours lieu à des débats intéressants sur les réseaux sociaux et à de riches comptes-rendus. La treizième édition s'est déroulée à Amsterdam durant l'été 2014 : https://petsymposium.org/2014/program.php

Le site communautaire Reddit comporte plusieurs sections où sont discutées et débattues les nouveautés, les bonnes ou mauvaises pratiques et les actualités en matière de vie privée, d'anonymat et de protection de l'identité, notamment reddit.com/r/Privacy, reddit.com/r/vpn, reddit.com/r/technology, reddit.com/r/netsec ou pay.reddit.com/r/darknetplan.

# 10 Quel avenir pour l'anonymat ?

*Comme le dit le journaliste Jean-Marc Manach, il ne faut pas non plus confondre surveillance et transparence. Si la transparence, c'est la liberté de ne dire de soi que ce que l'on veut, alors la surveillance représente exactement l'inverse : c'est la négation de cette liberté*[191].

Il est difficile d'apporter une conclusion définitive à ce guide : les techniques évoluent très vite et la question est fréquemment chamboulée, tant par les géants du Web que par les États. Entre la première et la seconde édition de cet ouvrage (que vous tenez entre les mains), un certain Edward Snowden a fourni à plusieurs médias des détails sur la NSA de toute première importance pour comprendre la surveillance qui s'exerce sur Internet et les moyens techniques qui y sont consacrés.

Il est en tout cas certain que jamais les inquiétudes vis-à-vis de l'identité et de la vie privée sur Internet n'ont été aussi aiguës. Les entreprises et les organisations se positionnent toujours plus nombreuses sur ce créneau, proposant des extensions pour navi-

gateurs (chapitres 4 et 5), des solutions de VPN (chapitre 6) ou des applications tout-en-un pour les smartphones (chapitre 8). Pourtant, les gouvernements ne semblent pas prêts à relâcher leur emprise sur les réseaux, pas plus que les entreprises et autres réseaux sociaux à cesser d'exploiter les données personnelles des internautes.

Nous espérons que ce livre vous aura donné quelques armes pour ne pas être les victimes collatérales de cette guerre qui fait rage.

## Des réformes s'annoncent

Paradoxalement, certains gouvernements s'intéressent de plus en plus près à la question de la protection de la vie privée de leurs citoyens.

Les autorités américaines poussent l'initiative Do Not Track, qui permettrait aux utilisateurs de signaler depuis leur navigateur leur souhait de ne pas être tracés et obligerait les entreprises publicitaires à en tenir compte. C'est un premier pas.

La Maison-Blanche, quant à elle, veut aller dans la direction d'un Privacy Bill of Rights qui comporterait sept droits : le contrôle individuel, la transparence, le respect du contexte, la sécurité, l'accès et l'exactitude, la collecte limitée et la responsabilité[192].

En France, François Hollande a promis un « habeas corpus numérique[193] » (qui prend parfois le nom plus sobre de « loi numérique »), dont les contours et l'éventuel calendrier d'adoption restent très flous. Au menu : une plus grande protection de nos données personnelles. La collecte et l'exploitation des données personnelles sont également dans le viseur d'un rapport sur la fiscalité numérique rendu début 2013[194]. La notion de droit à l'oubli, qui consisterait en la possibilité, pour les internautes, de faire effacer certaines de leurs données ou informations personnelles sur Internet est régulièrement

remise sur le tapis, mais extrêmement compliquée à mettre en place et à appliquer.

Tout récemment, une décision de la Cour de justice de l'Union européenne a confirmé que Google, en tant que moteur de recherche, était responsable des données personnelles contenues dans les pages qu'il indexe. La firme de Mountain View a donc été contrainte de mettre à disposition des internautes un formulaire de « droit à l'oubli »[195]. Il est accessible à l'URL suivante : https://support.google.com/legal/contact/lr_eudpa?product=websearch. Ce dernier a rencontré un très grand succès : lors de sa première journée de mise en ligne, 12 000 demandes ont été adressées par les internautes[196]. Le concurrent Bing a, dans la foulée, annoncé qu'il mettrait en place un dispositif similaire[197].

## Des pistes non étatiques

En dehors des États, des solutions et des réflexions commencent à émerger.

Les projets Midata au Royaume-Uni et MesInfos en France attaquent de front la question de la collecte et de l'exploitation de l'identité sur Internet[198].

Une piste souvent évoquée, notamment par les chercheurs, est celle de la séparation entre l'identification nécessaire sur Internet et ailleurs, et l'identification, c'est-à-dire la divulgation de données personnelles. Google n'a, par exemple, pas besoin de connaître notre véritable identité pour savoir que nous sommes intéressés par la musique celtique ou les voyages en Amérique du Sud. Cela reste une idée très théorique, incarnée notamment par le projet de **carte d'identité blanche électronique** du chercheur Yves Deswarte[199], qui permettrait de justifier de ses droits (de prendre un avion par exemple), sans avoir à divulguer d'informations personnelles.

**Fiction Une société complètement anonyme ?**

Andy Greenberg, dans son livre *This Machine Kills Secrets*, raconte comment les « cypherpunks », ces hackers pionniers des technologies de cryptographie et d'anonymat, ont imaginé une véritable dystopie en se demandant à quoi ressemblerait une société où l'anonymat serait total. Elle serait bien différente de la nôtre : il y serait extraordinairement facile de publier des secrets industriels ou étatiques. Ce ne serait pas une société sans secrets, mais une société où ne subsisteraient que les secrets privés et individuels, tandis que toute information concernant une organisation ou un État aurait de très grandes chances de devenir publique. C'est une bonne illustration de la nature ambivalente de l'anonymat.

D'autres idées peuvent être avancées, comme un droit au mensonge ou un droit à s'équiper de logiciels protégeant son identité[200].

## La solution par les entreprises ?

Le commerce de la vie privée est en pleine extension. Internet et ses acteurs veulent s'autoréguler, dans un monde numérique où le modèle économique basé sur l'échange de données personnelles contre des services a pris le dessus. Cet échange, apparemment équilibré, n'est d'ailleurs peut-être pas aussi avantageux qu'il en a l'air. Étant donné que nous n'avons aucun moyen de savoir quel effet peut avoir la divulgation de nos données dans un futur éloigné, il est impossible de jauger les véritables enjeux derrière cet accord tacite. Pourtant, on l'a vu, il est difficile de l'éviter si on veut utiliser Internet aujourd'hui.

Cependant, les entreprises pourraient apporter une solution crédible et durable à la question de la vie privée. Selon le juriste Lawrence Lessig, il y a quatre moyens de réguler le cyberespace : les normes, les lois, le code et le marché. Selon Cory Doctorow, intellectuel américain, écrivain, penseur et défenseur infatigable

des droits numériques, seuls les deux derniers peuvent apporter une solution à la protection de la vie privée[201].

### Défense Les ONG qui défendent la vie privée

**En plus des ressources évoquées dans le chapitre précédent, il nous faut mentionner les nombreuses associations et autres ONG qui défendent la vie privée, notamment en ligne : l'Electronic Frontier Foundation (EFF), Privacy International (PI), le Center for Democracy and Technology (CDT), l'Electronic Privacy Information Center (EPIC), Front Line Defenders ou l'European Digital Rights (EDRi).**
**En France, la voix des internautes sur ces sujets est notamment portée par La Quadrature du Net.**

Les normes ne peuvent pas fonctionner : on alerte sans cesse sur les dangers que feraient peser les réseaux sociaux sur la vie privée et on multiplie les caméras de vidéosurveillance. On sensibilise (parfois de manière très peu subtile) les enfants sur les dangers de Facebook, mais on continue à vendre toujours plus de logiciels permettant de les surveiller et de contrôler leur usage des technologies numériques. Doctorow balaie également les lois, qui pourraient pourtant donner plus de droits aux utilisateurs sur leurs données : « S'il y a une chose que quinze ans de batailles législatives autour d'Internet nous ont apprise, c'est que rien n'est jamais vraiment réglé en assignant des droits de propriété à une information copiable à l'infini », assène-t-il.

En revanche, pour lui, la solution peut venir des marchés. Il rappelle notamment que Mozilla a rencontré le succès avec Firefox, notamment parce que c'était le premier navigateur à bloquer les pop-ups, au grand dam des publicitaires. Cette fonctionnalité a depuis été généralisée à tous les navigateurs. Pourquoi un navigateur respectant la vie privée par défaut ne rencontrerait-il pas un large succès, entraînant par capillarité tous les autres navigateurs et changeant les comportements

des publicitaires et des entreprises ? On pourrait également, dit-il, imaginer un système d'exploitation pour mobile qui « mente » aux applications avides de données (faux numéro de téléphone, fausse localisation, etc.). D'autant que, défend-il, si au lieu d'aspirer continuellement de larges quantités de données personnelles, les entreprises ciblaient davantage leurs efforts et obtenaient l'assentiment du consommateur, les perspectives publicitaires seraient bien plus juteuses !

Poussées par l'appel d'air créé par les révélations Snowden, de nombreuses entreprises se sont mises à proposer des solutions pour protéger sa vie privée, ou au moins à utiliser cet argument comme élément de leur communication.

Il ne vous aura pas échappé que certaines technologies protectrices de l'anonymat et de la vie privée sont extrêmement complexes. Encore aujourd'hui, les outils cryptographiques efficaces sont le plus souvent réservés à une élite disposant d'un temps et d'une habileté inaccessibles à la plupart des utilisateurs d'Internet. Par effet miroir, les outils les plus faciles d'utilisation sont souvent proposés par des entreprises exploitant les données personnelles et proches des services de renseignement.

Glenn Greenwald, le journaliste que Edward Snowden a choisi pour révéler les abus de la NSA, raconte souvent qu'il a failli passer à côté de l'affaire du siècle parce qu'il ne maîtrisait pas la cryptographie.

La piste qu'il semble intéressant d'emprunter, c'est de dépasser ce paradoxe et de construire des outils faciles à utiliser offrant une protection efficace. Développeurs, à vos lignes de code !

## Vous avez dit démocratie ?

Au-delà d'un enjeu strictement technique et économique, la question de l'anonymat sur Internet oblige à aborder des

notions aussi cruciales que la vie privée, l'identité en ligne et les libertés. Et, en filigrane, celle de la démocratie.

### Fiction **Une vie de données**

**Certains imaginent déjà à quoi pourrait ressembler un futur où nos données personnelles, y compris les plus intimes, seraient publiques et disponibles pour les entreprises. Une nouvelle[202], parmi d'autres, a rencontré un certain succès. On y lit l'histoire d'un homme qui veut commander une pizza. Problème : le livreur refuse ! En effet, il a détecté chez le client un problème de cholestérol en ayant accès à ses données médicales. Le livreur lui propose également un bon de réduction pour ses prochains achats de préservatifs, ses données bancaires révélant qu'après sa journée de travail, il n'était pas rentré chez lui, mais chez sa maîtresse…**
**À court terme, pourquoi un employeur se refuserait-il à acquérir vos données de navigation ou un accès à votre activité sur les réseaux sociaux pour mesurer votre productivité, votre propension à la maladie ou la probabilité que vous tombiez enceinte[203] ?**

Pour l'avocat Michel Benichou[204], cette protection de l'identité révèle ni plus ni moins que la « maturité démocratique » d'une société et la force du lien de confiance entre un État et ses citoyens : protégez-vous, choisissez la manière dont vous voulez apparaître et être connus, nous vous faisons confiance pour ne pas abuser de cette liberté.

Cette marge de liberté, bien loin de la transparence absolue que voudraient coller à Internet certains idéologues, nous semble vitale, même si les usages frauduleux et immoraux en sont le revers de la médaille. « Dans une démocratie, je considère qu'il est nécessaire que subsiste un espace de possibilité de fraude. Si l'on n'avait pas pu fabriquer de fausses cartes d'identité pendant la guerre, des dizaines de milliers d'hommes et de femmes auraient été arrêtés, déportés, sans doute morts. J'ai toujours été partisan de préserver de minimum d'espace sans lequel il n'y a pas de véritable démocratie », écrit par exemple Raymond Forni, ancien président de la Cnil et ex-président socialiste de l'Assemblée nationale[205].

De plus, la définition même de la vie privée (voir le chapitre 1), lie fortement cette dernière à la question de la démocratie. Pour l'universitaire Jack Hirshleifer, la vie privée est « le désir humain d'indépendance par rapport aux autres, de contrôler sa propre personne et son propre temps[206] ». Pour la juriste Ruth Gavison[207], la vie privée n'est rien d'autre qu'un moyen de susciter « la promotion de la liberté, l'autonomie, l'individualité, les relations humaines et, plus fondamentalement, l'existence d'une société libre ». C'est le fondement même de nos sociétés démocratiques.

## Les effets néfastes de l'anonymat ?

La question politique n'est jamais loin et les effets d'une chasse trop poussée faite à l'anonymat a également de quoi questionner. Comment feront les forces de l'ordre pour traquer les véritables méchants d'Internet lorsque tout le monde sera contraint à masquer son identité à l'aide de technologies sophistiquées ? Les premiers chiffres sont là : après que leur pays a adopté les premières lois pro-copyright s'appliquant à Internet, les jeunes Suédois se sont rués sur les VPN[208].

Plus les technologies anonymisantes seront répandues et utilisées, plus les gouvernements seront enclins à pousser la surveillance des réseaux et des internautes, dans un véritable cercle vicieux où ne sortiraient gagnantes que les entreprises, et certainement pas les internautes. D'où peut-être la nécessité, pour le pouvoir politique, de protéger l'identité de ses citoyens afin qu'ils ne soient pas contraints de le faire eux-mêmes… même si ce livre est là pour vous donner quelques armes.

De même, que serait le journalisme d'investigation sans le contre-pouvoir de plus en plus puissant que constituent les *whistleblowers* – ces employés et fonctionnaires qui mettent en pleine lumière les turpitudes de leurs employeurs –, sans la protection de l'identité et de l'anonymat[209] ?

## Le double jeu des politiques

La dissonance permanente qu'entretiennent les pouvoirs politiques sur ces questions n'aide pas à une compréhension claire des enjeux. Internet est présenté tour à tour, parfois par les mêmes acteurs, comme un vaste espace public où les internautes ont perdu tout sens de la vie privée, voire comme une jungle où les lois sont inapplicables et où les criminels anonymes prospèrent.

Ceux qui alertent fréquemment sur les méfaits de Facebook sur la vie privée (ils n'ont pas complètement tort) passent bien souvent sous silence le comportement de certaines entreprises collectant et exploitant des montagnes de données personnelles, parfois sans le consentement des internautes. Parallèlement, et sans avoir peur de leurs propres contradictions, les États multiplient les lois qui accroissent le contrôle d'Internet et de l'identité des internautes, développent la vidéosurveillance, la biométrie et les politiques sécuritaires en tout genre. Ils justifient parfois de manière totalement fallacieuse cette évolution par la propension supposée des internautes à s'exposer sans limite en ligne !

Les États ne doivent pas seulement s'emparer de la question du point de vue de la loi. L'affaire Snowden a montré que certains d'entre eux, et parmi les plus puissants, s'étaient engagés dans une entreprise de démolition des dispositifs de sécurité sur Internet. Une plus grande transparence sur les agissements des grandes centrales de renseignement et de certaines entreprises associées ne pourrait que bénéficier à tous : au risque de vouloir un Internet toujours plus risqué pour les criminels et les terroristes, les grandes démocraties risquent de se retrouver avec un Internet hostile pour tous.

Que peuvent faire en réalité les politiques ou les entreprises face à la nature même des ordinateurs et d'Internet, qui sont avant tout des machines à copier ? Que vont alors devenir

toutes les données que certains d'entre eux ont accumulées par terabits entiers ? Il n'y a en fait aucun moyen de le savoir, pas plus que les éventuels dégâts qu'une recherche Google ou une discussion sur un service de messagerie instantanée pourraient occasionner si elles venaient à refaire surface dans quelques années. L'embarras causé par la ré-émergence d'une poignée de statuts Facebook vieux de cinq ans seulement laisse entrevoir ce problème[210]. « Les humains sont incroyablement mauvais pour évaluer une action lorsque ses conséquences surviendront dans le futur », écrit Cory Doctorow[211]. Derrière cette affirmation, voyez un avertissement : si vous ne vous intéressez pas à votre vie privée, celle-ci risque bien de s'intéresser à vous dans un futur pas si lointain.

C'est parce que la vie privée et la vie publique cohabitent intensément, séparées seulement par un clic ou par un mot de passe, que ces concepts sont si difficiles à appréhender. Nous espérons que ce livre aura permis de percevoir et d'appliquer certaines limites.

## Renversement de paradigme

Plus qu'une évolution, Internet induit un changement radical. Auparavant, un individu avait la plupart du temps une vie privée et parfois une vie publique. Cet équilibre est d'ailleurs reflété dans la loi française, qui impose généralement la justification de la levée de l'anonymat. Internet et plus généralement les technologies de surveillance (vidéosurveillance, biométrie) tendent à un renversement : notre vie devient de plus en plus publique par défaut.

### Initiative Une solution radicale : le réseau « pirate »

**Pour protéger l'anonymat des internautes, des initiatives peu communes fleurissent, comme le réseau Commotion, dont le principe est simple : des ordinateurs se connectent entre eux, sans passer par Internet, pour former un réseau autonome, décentralisé et à l'abri des velléités diverses de surveillance[212]. Les « pirate box », mini-serveurs portatifs permettant à n'importe quel ordinateur de s'y connecter et de déposer ou de télécharger des fichiers, se multiplient également.**

Au fond, il n'y a nul besoin d'être alarmiste quant à ce changement. Sur Internet, si on ne s'intéresse pas particulièrement à vous, vous êtes anonyme. Pour la plupart d'entre nous, Internet reste un lieu où il est facile d'être un parfait inconnu vis-à-vis des autres et c'est sans doute une des raisons fondamentales de son succès. Cependant, pour une machine, un État, une entreprise, ou simplement quelqu'un d'un peu curieux, vous n'êtes jamais anonyme.

Ce renversement entre vie privée et vie publique n'est en outre pas négatif par nature. Ces vies ne sont pas incompatibles et sont toutes les deux bénéfiques. Il ne faut pas non plus avoir peur d'Internet parce que votre vie privée y serait menacée. Comme le dit bien le journaliste Jean-Marc Manach, un des meilleurs observateurs de ces sujets, on pouvait avoir, avant Internet, une discussion privée dans un lieu public (un café par exemple) et ce n'est parce que la vie sexuelle augmente le risque de maladies vénériennes qu'il faut refuser de faire l'amour[213]!

Les idées d'anonymat et de vie privée n'ont jamais été aussi pertinentes pour analyser les relations sociales. Elles trouvent de nouvelles formes, se déplacent, se reconfigurent. On peut être « public » dans certains domaines, anonyme dans d'autres. La vie privée, ce n'est rien d'autre que la capacité de (dé)limiter en toute liberté ces deux sphères. Toutefois, la lutte pour les préserver est de plus en plus ardue et technique. Le combat est d'autant plus crucial qu'il est maintenant

impossible de se tenir loin d'Internet, tant la vie se déroule dans sa Toile.

# 11 Entre la chaise et le clavier

*En informatique, on a coutume de dire que la majorité des problèmes vient de ce qui se situe entre la chaise et le clavier, c'est-à-dire de l'utilisateur. De même, en matière d'anonymat, il est possible d'intervenir à ce niveau, sans outil ni logiciel particuliers.*

Comme nous le disions au chapitre 5, en matière de discrétion sur les réseaux, de nombreux problèmes peuvent être évités et beaucoup de précautions mises en place en prenant simplement du recul sur son utilisation d'Internet et en adoptant de petits réflexes très simples.

On listera quelques principes de base, applicables à notre sujet, mais également à toute forme de sécurité informatique.

Culture **« L'interface chaise-clavier »**

**Dans le jargon des informaticiens, l'utilisateur est parfois appelé « l'interface chaise-clavier ». On parle même de « Code 45 » (ou Code 18), 45 centimètres (18 pouces) étant la distance moyenne entre un écran et l'utilisateur[214]. Si, après vous avoir écouté expliquer votre problème, un informaticien vous répond qu'il y a un bogue dans l'interface chaise-clavier, vous saurez qu'il se moque gentiment de vous.**

## Ne jamais faire confiance

Il ne faut jamais faire une confiance aveugle et définitive à un programme ou à un outil informatique. Ce n'est pas parce qu'il est fait de 1 et de 0 qu'il est infaillible, ou qu'il fonctionnera demain comme il a fonctionné aujourd'hui.

De manière générale, il faut toujours utiliser son cerveau en premier. Aucun logiciel n'est parfait et idéal pour votre situation. L'intérêt n'est pas d'installer des logiciels sans comprendre. C'est même le meilleur moyen pour instaurer un faux sentiment de sécurité et se faire piéger... Il s'agit de maîtriser leurs points forts et, surtout, leurs points faibles, pour adapter leur utilisation à votre situation.

## Comparer les coûts et les risques et s'adapter en fonction

Pour se protéger sur Internet, comme pour se protéger dans le monde physique, il s'agit toujours de comparer les coûts et les risques des outils utilisés ou des pratiques à mettre en œuvre. Les logiciels qu'on utilise pour se prémunir contre la surveillance de sociétés privées qui revendent nos données personnelles ne sont pas les mêmes que ceux que certains peuvent utiliser pour échapper à une surveillance d'État.

PARANOÏA **Qui nous surveille ?**

Comme le dit le dicton, même les paranoïaques ont des ennemis. Proposons une alternative : contrairement à ce que l'on pourrait penser, même les paranoïaques sont surveillés !

Et même ceux qui ne sont pas paranoïaques, d'ailleurs. Que ce soit votre employeur, votre conjoint, vos parents, vos enfants, les multiples entreprises qui glanent et revendent vos données personnelles, les services commerciaux que vous utilisez tous les jours sur Internet, votre fournisseur d'accès à Internet, des fonctionnaires – pas forcément malveillants – de votre État, le client suivant du cybercafé, vos concurrents, vos collègues, vos confrères, les services de renseignement d'un pays ou les services informatiques d'une entreprise, la surveillance du réseau se niche un peu partout.

Il n'est nul besoin d'être un dissident politique ou un journaliste d'investigation pour que nos actions sur Internet intéressent un certain nombre de personnes.

Certains outils peuvent offrir une protection très satisfaisante, mais attirer l'attention sur vos activités. Certaines techniques et outils induisent des contraintes en termes de technicité et de temps qui peuvent ralentir votre navigation et votre travail. Ainsi, le niveau de protection et de précaution que l'on s'accorde doit toujours être fonction des objectifs que l'on se donne en termes de sécurité et de risques encourus.

On pourra faire la comparaison avec une serrure : si vous habitez au sixième étage dans une ville tranquille et si vous ne menez aucune activité politique, investir dans un verrou très onéreux, très complexe et long à ouvrir ainsi que dans une porte blindée, même si le niveau de protection est excellent, sera peut-être contre-productif en termes de coût, de temps et de complexité… sauf si vous estimez courir des risques.

## Internet n'est pas fait pour l'anonymat

Pour maximiser les chances de parvenir à être anonyme, sinon discret, sur Internet, il convient de savoir comment fonc-

tionne, à grands traits, le réseau. On partira d'un postulat simple : sur Internet, les données circulent en clair, aux yeux de tous, pour peu que l'on sache où regarder.

Idée reçue **Il n'y a pas d'anonymat sur Internet**

**Thomas Drake est un ancien agent de la NSA, l'agence américaine chargée du contre-espionnage, de la cryptographie et de la surveillance des réseaux. Au milieu des années 2000, cet expert a voulu dénoncer un certain nombre d'abus commis par son agence.**
**Pour ce faire, il a dû entrer en contact, anonymement, avec des journalistes. Il savait, par son métier, que c'était un véritable défi. Voilà ce qu'il dit aujourd'hui : « Il n'y a pas d'anonymat électronique absolu. Il y a des moyens de rendre plus difficile votre identification. Mais il y a toujours une piste numérique[215]. »**

Internet n'est pas conçu pour l'anonymat. Lors de sa création, la problématique était de permettre à des réseaux essentiellement universitaires parlant des langages différents de communiquer entre eux. Très vite, des protocoles ouverts ont été définis et les informations transitaient de serveur en serveur en clair, sans être chiffrées[216].

Aujourd'hui, Internet, ce sont des ordinateurs qui parlent avec des ordinateurs. S'y connecter, c'est donc relier son ordinateur à des milliers d'autres, qui échangent des informations, qui se « parlent », qui s'aiguillent et se dirigent les uns les autres vers d'autres ordinateurs encore, qui contiennent (hébergent) le site Internet auquel vous désirez accéder...

Puisqu'il faut savoir où renvoyer les données demandées, tous ces échanges sont autant de traces de toutes vos connexions. Tous les intermédiaires gardent vos traces : l'hébergeur du site, votre fournisseur d'accès à Internet et, plus généralement, tous les ordinateurs qui se trouvent entre vous et les sites que vous visitez.

### Adresse Une histoire d'IP

Un des principaux éléments qui permettent de vous identifier sur le réseau est votre adresse IP. Cet identifiant (quasi) unique est associé à chaque appareil – ordinateurs, téléphones, sites web – connecté à Internet et, parmi d'autres dispositifs, permet aux machines de dialoguer entre elles et de transmettre des informations.
Imaginons que vous vouliez accéder au site trucmuche.fr. Vous allez d'abord demander à votre fournisseur d'accès quelle adresse IP correspond à ce nom de domaine. Pour cela, votre FAI va avoir recours à un autre intermédiaire, un serveur DNS, qui va établir la correspondance entre « trucmuche.fr » et l'adresse IP du site, qui va permettre à votre ordinateur d'y parvenir.
Et vous n'avez pas fini de laisser des traces : une fois arrivé sur le site, vous laissez immanquablement votre adresse IP sur son serveur. Il est ensuite aisé pour l'administrateur du site de retrouver – de son propre chef ou si la justice le lui demande – une adresse IP correspondant à une connexion (ou à un commentaire sur un site par exemple). Votre FAI est ensuite capable de dire à qui appartient cette adresse IP.

Le problème de la confidentialité des échanges qui se pose aujourd'hui n'est pas nouveau : il existait déjà pour le téléphone ou le courrier postal d'une personne surveillée. Il y a néanmoins une différence fondamentale : il est beaucoup plus facile de surveiller quelqu'un à l'ère numérique.

Si un individu utilise les moyens de communication traditionnels (courrier, téléphone), il faut mobiliser beaucoup plus de ressources pour aboutir à un résultat similaire en termes de surveillance[217]. Contrairement à ce que l'on entend fréquemment, c'est la surveillance, bien plus que l'anonymat, qui est facilitée par les nouvelles technologies.

Heureusement, Internet et les nouvelles technologies en général proposent autant de solutions qu'elle comportent de vulnérabilités.

# Comment choisir ses armes ?

De nombreux logiciels apparaissent et disparaissent en permanence. Il vous faudra donc sans doute un jour utiliser des logiciels ou des outils qui ne sont pas présentés ici. Mieux vaut vous donner les clefs pour choisir vos armes qu'un conseil périssable. Voici les quelques questions qu'il faudra vous poser pour choisir un logiciel et déterminer si vous pouvez lui faire confiance[218].

## Choisir des outils utilisés par une large communauté d'utilisateurs

Il faut que l'outil ou le logiciel soit utilisé par un ensemble varié d'utilisateurs. Plus la population des utilisateurs sera variée, plus il sera facile de se fondre dans la masse et plus il sera difficile pour un tiers de savoir qui vous êtes. Prenons l'exemple de Tor : il est utilisé à la fois par des activistes qui veulent contourner la censure qu'ils subissent dans leur pays, des particuliers, des journalistes, mais également par des militaires ou des officiels gouvernementaux. Utiliser Tor ne donne donc que peu d'indices sur votre identité.

### Histoire Tor : entre l'État et les activistes

Comme beaucoup d'innovations technologiques, Tor est issu de l'armée américaine, plus particulièrement de l'organisme de recherche de la marine et de celui du département de la défense, la DARPA (qui est également à l'origine d'Internet). Deux personnes ont participé à ses premiers développements : Paul Syverson et Roger Dingledine.
Les services de renseignement américains l'utilisent, tout comme les services de police français (des armées et des forces de l'ordre du monde entier y ont également recours). Le crime (pédopornographie, vente d'armes) y fait également florès. De nombreuses entreprises, enfin, ou firmes d'intelligence économique l'utilisent pour surfer en toute discrétion sur les sites de leurs concurrents.

En revanche, le simple fait de recourir à un outil ou à un logiciel qui est utilisé par un nombre restreint d'utilisateurs, outre le doute que cela doit susciter en termes de fiabilité du logiciel, donne de sérieux indices sur votre identité.

Il faut également se poser la question de la date de création d'un logiciel : lorsqu'un logiciel est assez récent et sa diffusion encore restreinte, le type d'utilisateurs est plus homogène (en termes de langue, de pays, d'activité). Il est plus facile de savoir qui utilise un logiciel lorsque celui-ci est récent et encore peu répandu.

Un outil ou un logiciel efficace doit pouvoir être utilisé à long terme. Le problème, c'est que le développement d'un logiciel est complexe, coûteux et peut s'arrêter très facilement. Cela est plus difficile s'il existe autour de ce logiciel une large communauté de bénévoles ou une organisation qui se charge du développement du logiciel et de son assistance technique.

### Chiffres **Tor, l'outil le plus commun**

**On trouve un certain nombre de statistiques, notamment à l'adresse :**

**> https://metrics.torproject.org/**

**En seulement trois ans, le nombre de relais Tor a doublé, passant de 1 500 en 2009 à plus de 3 000 à la fin de l'année 2012. Le nombre d'utilisateurs, sur la même période, a quant à lui été multiplié par 5, de 100 000 à plus de 500 000 utilisateurs quotidiens.**

L'exemple de Tor est très parlant. Ce réseau s'appuie sur un large maillage de bénévoles très impliqués, développeurs ou simples internautes, qui assurent la survie et le développement du logiciel. Cela permet d'envisager l'utilisation du logiciel à long terme. Par ailleurs, une communauté nombreuse est plus à même de répondre à vos éventuelles questions ou difficultés avec les outils.

## Utiliser des logiciels libres

Il conviendra également de préférer les *logiciels libres*.

**OPEN Les quatre libertés du logiciel libre**

Pour être qualifié de libre, un logiciel doit réunir quatre principes. L'utilisateur doit être libre d'utiliser le logiciel pour quelque usage que ce soit. Il doit pouvoir accéder au code source du programme pour l'étudier et éventuellement l'adapter à ses besoins. Il doit aussi pouvoir distribuer librement des copies de ce programme. Enfin, l'utilisateur doit être en mesure d'améliorer le programme et de diffuser ces améliorations librement[219].

Même si les utilisateurs se soucient généralement peu de ces libertés, ces dernières jouent un grand rôle dans la fiabilité d'un logiciel, à plus forte raison quand celui-ci a été largement diffusé.

La raison est simple : si un logiciel est libre, alors il y a de fortes chances (pas toujours, il convient donc de le vérifier) que ce dernier ait été inspecté dans tous ses recoins par des informaticiens. C'est particulièrement important dans le cas de logiciels protégeant l'identité de ses utilisateurs, où une faille, un défaut de sécurité ou une « porte dérobée » peuvent compromettre leur anonymat et leur sécurité. Ce genre de chausse-trappes est plus facilement décelé lorsque le code peut être modifié et diffusé.

**EXEMPLE Le FBI voudrait une porte dérobée**

La police fédérale américaine a fait pression sur les éditeurs de logiciels et de services de la Silicon Valley pour que ces derniers introduisent dans leurs services des *backdoors*, c'est-à-dire des portes dérobées permettant d'espionner plus facilement les échanges entre utilisateurs[220]. Ce genre de choses a moins de chance de survenir avec un logiciel libre : cette porte serait immédiatement repérée et refermée.

De plus, ces logiciels n'ont pas de but lucratif et ne répondent donc pas à des exigences de rentabilité et de concurrence, mais d'efficacité et de fiabilité.

Plus que libre, le logiciel doit également être accompagné de ce qu'on appelle une documentation, si possible riche et complète. C'est une sorte de manuel d'utilisation du code du logiciel, qui précise les buts recherchés par son concepteur et les moyens d'y parvenir. Autant d'indices et d'aides précieuses pour les développeurs qui voudraient contribuer et rendre le logiciel plus sûr et plus fiable.

Les logiciels libres ou open source maintenus par de petites équipes, restreintes et parfois secrètes, souvent sans grand moyens financiers, sont plus fragiles et peuvent voir leur développement arrêté, comme c'est le cas avec le logiciel de chiffrement TrueCrypt[221]. Parfois, le fait que ce soit des petites équipes rend l'erreur plus facile et l'ouverture du code ne suffit pas à repérer l'erreur rapidement : ainsi, la faille Heartbleed a été insérée faute d'une relecture suffisante du code et a subsisté pendant plusieurs mois[229].

PARADOXE **Logiciel ouvert, logiciel plus sûr ?**

**On pourrait penser qu'avec un code ouvert et libre, les gouvernements, les entreprises et les individus mal intentionnés pourront mieux détecter les failles et les exploiter, voire en introduire de nouvelles. C'est un risque, mais pour toutes les raisons précédentes, les bénéfices de l'ouverture et de la liberté sont bien plus grands que leurs inconvénients. Selon Roger Dingledine[223], un des informaticiens à l'origine du projet Tor, les logiciels libres ont une évolution technologique plus rapide que les logiciels dits propriétaires.**

## Sélectionner une infrastructure décentralisée

Il vaut mieux choisir une solution qui repose sur une infrastructure décentralisée. L'exemple peut encore une fois être celui de Tor : si un des ordinateurs impliqués dans le projet est

compromis ou est débranché, cela n'affecte que très marginalement la force et l'intégrité de tout le réseau. Comme Internet, qui repose sur des millions de réseaux interconnectés entre eux, un service sera d'autant plus robuste et résistant en termes de protection de l'identité qu'il reposera sur des fondations éparpillées : si vous concentrez toutes les données des utilisateurs en un seul endroit, il sera plus facile d'y accéder et de mettre à bas leur anonymat d'un seul coup.

## Méfiez-vous des entreprises

Méfiez-vous des entreprises et des services qu'elles proposent, quelles qu'elles soient ! Elles auront toujours un intérêt commercial qui sera plus important que la sauvegarde de vos libertés et la protection de votre anonymat. Les conditions de stockage de vos données et de vos fichiers sur les serveurs des différentes entreprises et services que vous utilisez sont variables. Certains experts ont une position radicale et estiment qu'il faut partir du principe que ce qui est hébergé en ligne ne vous appartient plus.

Sans parler de cette somme colossale de données personnelles récoltées, les logiciels créés, développés et maintenus par des activistes ont tendance à être plus sûrs et plus robustes, notamment vis-à-vis des demandes de l'État.

**Fiabilité** **Quelle entreprise vous couvre ?**

L'association américaine Electronic Frontier Foundation a demandé à plusieurs grandes entreprises du Web quelle était leur politique vis-à-vis des demandes gouvernementales. Quatre questions ont été posées à chaque entreprise pour les classer. Avertit-elle l'utilisateur quand le gouvernement l'interroge à son sujet ? Est-elle transparente vis-à-vis des requêtes gouvernementales ? Se bat-elle devant les tribunaux pour protéger les données personnelles de ses utilisateurs ? Se bat-elle devant le Congrès pour ces données personnelles ? Les résultats sont éloquents[224].

Qui mieux que Eric Schmidt, le patron de Google, pour expliquer cela ? « Nous pouvons mettre vos données à l'abri de tout le monde, sauf du gouvernement et de ses injonctions légales. Si le gouvernement viole votre vie privée et si cela ne plaît pas, il faut en parler avec votre représentant au Congrès[225]. »

Il est conseillé aussi de lire les conditions générales d'utilisation (les textes qui codifient l'usage que vous pouvez faire d'un service) des logiciels ou des services que vous utilisez. On a parfois de belles surprises ! On notera enfin que tout logiciel ou service hébergé aux États-Unis est soumis aux diverses lois permettant à la NSA de piocher dans les données personnelles, notamment le « Patriot Act », extrêmement invasif en termes de confidentialité et de vie privée[226]. De plus, la NSA intercepte aussi une masse colossale de données en dehors de toute juridiction (voir chapitre 2).

EXEMPLE **Le proxy trahit les Anonymous**

**Un certain nombre de membres du collectif Anonymous utilisaient un service de VPN, Hidemyass. L'identité de plusieurs d'entre eux a été compromise lorsque l'entreprise qui gérait le VPN a reçu un mandat de la justice britannique[227].**

# Identifier votre « ennemi »

Les outils n'ont pas tous la même finalité, les mêmes points forts et points faibles. Il faut donc les utiliser à dessein. Un bon exemple peut être celui de la mésaventure survenue en novembre 2012 à David Petraeus.

Le directeur de la CIA, David Petraeus, entretenait avec Paula Broadwell une relation extraconjugale. Sa maîtresse et lui avaient pris toutes les précautions pour se protéger de son épouse, notamment vis-à-vis de leur correspondance électronique. Ils échangeaient des messages en passant par le dossier

*brouillon* d'une boîte mail commune. La technique fonctionnait parfaitement pour dissimuler à sa femme les messages reçus et envoyés.

Le danger (et leur perte) est venu d'un autre adversaire, qu'ils n'attendaient pas : le FBI, qui avait identifié un compte e-mail, apparemment anonyme, envoyant des messages menaçants à une tierce personne. Le FBI, plus redoutable encore que la conjointe trompée, a obtenu les logs de connexion auprès du fournisseur d'e-mail (et donc l'adresse IP qui avait été utilisée pour y accéder) et a demandé quels autres comptes la même adresse IP avait visités. Il a ainsi obtenu l'adresse d'un compte anonyme – et tous ses contenus, y compris les brouillons échangés avec David Petraeus. On avait accédé à ce compte depuis plusieurs adresses IP différentes, mais toutes venaient de Wi–Fi publics d'hôtels. Il a suffi au FBI d'identifier les hôtels en question, de croiser les noms qui y avaient fait une réservation… et d'arriver à Paula Broadwell.

Si les deux protagonistes avaient protégé leur adresse IP (voir le chapitre 7), le FBI n'aurait même pas pu identifier la boîte mail commune. Une autre précaution simple aurait compliqué la tâche des enquêteurs : accéder aux comptes e-mails depuis un VPN ou utiliser Tor (voir le chapitre 7).

### Expert Comprendre la menace

Matthew Blaze est chercheur en informatique à l'Université de Pennsylvanie et spécialiste en sécurité et en cryptographie. Il dit : « Comprendre une menace est toujours la partie la plus difficile de la sécurité informatique. S'ils [le général Petraeus et sa maîtresse, *ndlr*] avaient pensé que la menace viendrait du gouvernement, qui peut accéder à toutes les informations en demandant aux entreprises qui fournissent des services, et non de leurs époux, ils auraient sans doute agi différemment[228]. »

Les outils à utiliser ne sont pas les mêmes selon que vous voulez vous protéger des entreprises, des gouvernements, de votre patron ou de votre conjoint.

## L'erreur humaine et l'entraînement

Rappelons que la caractéristique de cette interface chaise-clavier, c'est sa propension à appuyer sur le mauvais bouton et, plus généralement, à commettre toutes sortes d'erreurs.

La sécurité est une chaîne, dont la force est égale à celle de son maillon le plus faible : si un seul des maillons casse, c'est toute la sécurité qui est compromise. Vous pouvez utiliser toute une série de logiciels très sophistiqués, mais si vous oubliez votre ordinateur ouvert dans un lieu public, cela met à bas tous vos efforts.

Même si la nécessité ne se fait pas sentir immédiatement, il vaut donc mieux utiliser fréquemment les logiciels conseillés dans cet ouvrage et s'entraîner à les manipuler. Ainsi, en cas de besoin, leur utilisation est devenue une routine, minimisant le risque d'erreur. Les logiciels facilitant l'anonymat sont parfois lourds et complexes : apprendre à s'en servir avant d'en avoir réellement besoin est un gage de sécurité.

On peut prendre toute une quantité de mesures de protection, mais selon Dan Kaminski[229], un chercheur spécialisé en sécurité informatique, « tout est artificiel, tout est enregistré. La réalité, c'est que si vous ne voulez pas que quelque chose apparaisse en première page du New York Times, alors ne le dites pas sur Internet ».

# Notes de fin

1. https://about.twitter.com/fr/company/
2. http://www.lemonde.fr/technologies/article/2012/10/04/facebook-franchit-la-barre-du-milliard-d-utilisateurs_1770255_651865.html
3. http://www.nielsen.com/us/en/insights/news/2012/buzz-in-the-blogosphere-millions-more-bloggers-and-blog-readers.html/
4. [Merzeau, 2009]
5. [Enguehard & Panico, 2010]
6. http://www.socresonline.org.uk/7/2/stalder.html/
7. [Brim & Ruebhausen, 1965] cités dans [Rochelandet, 2010].
8. [Rochelandet, 2010]
9. [Bok, 1989] citée dans [Rochelandet, 2010].
10. [Rochelandet, 2010]
11. Cette chercheuse américaine, l'une des plus écoutées sur les questions numériques, notamment celles qui touchent aux adolescents, insiste pour que l'on écrive son nom en minuscules. Pour comprendre les raisons de son choix, rendez-vous sur : danah.org/name.html.
12. Citée dans [Manach, 2010].
13. *Ibid.*

14.[Rallet & Rochelandet, 2010]
15.[Rallet & Rochelandet, 2010]
16.[Rallet & Rochelandet, 2010]
17.http://www.socresonline.org.uk/7/2/stalder.html/
18.http://www.zephoria.org/thoughts/archives/2010/01/16/facebooks_move.html/
19.https://help.riseup.net/fr/security/
20.[Manach, 2010]
21.http://www.guardian.co.uk/technology/2012/apr/19/online-identity-authenticity-anonymity/
22.[Lecomte, 2010]
23.http://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html
24.http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa/
25.http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html
26.http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
27.http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents
28.http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
29.https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/
30.http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life/
31.http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo/
32.http://www.lemonde.fr/pixels/article/2014/06/02/pourquoi-la-nsa-aspire-des-millions-de-photos-de-visages-sur-le-web_4429961_4408996.html
33.https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

34. http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html
35. http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html
36. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052#LEGIARTI000006529323/
37. http://owni.fr/2011/03/04/comment-le-fbi-le-ps-et-estrosi-ont-mis-le-net-sous-surveillance/
38. http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000024506075&cidTexte=LEGITEXT000006070987
39. http://bugbrother.blog.lemonde.fr/2012/04/12/les-gens-quon-arrete-cest-grace-a-internet/
40. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D36E11D2A9E96DD2D636FB0BE5BA55DD.tpdjo13v_2?cidTexte=JORFTEXT000000801164&categorieLien=id/
41. http://www.numerama.com/magazine/18191-la-lcen-a-enfin-son-decret-sur-les-donnees-a-conserver-par-les-hebergeurs.html/
42. http://ecrans.liberation.fr/ecrans/2011/12/23/1984-combien-ca-coute_953097
43. https://apps.opendatacity.de/stasi-vs-nsa/francais.html
44. http://archive.wired.com/wired/archive/13.08/tech.html
45. [Colin & Verdier, 2012]
46. http://www.le-tigre.net/marc-l.html
47. http://www.metafilter.com/95152/Userdriven-discontent#3256046/
48. http://powazek.com/posts/3250/
49. http://www.dailymail.co.uk/news/article-2019544/Facebook-director-Randi-Zuckerberg-calls-end-internet-anonymity.html/
50. http://pro.clubic.com/entreprises/google/actualite-611304-cnil-inflige-amende-150-000-google.html
51. http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php/
52. http://www.lemonde.fr/technologies/article/2011/06/29/google-le-concurrent-direct-de-facebook-debarque_1542282_651865.html
53. http://www.facebook.com/help/. Page consultée en septembre 2012.

54.[Manach, 2010]

55.http://www.guardian.co.uk/technology/2012/apr/19/online-identity-authenticity-anonymity/

56.[Merzeau, 2009]

57.https://www.schneier.com/essays/archives/2007/05/is_big_brother_a_big.html

58.online.wsj.com/article/SB10001424052748703940904575395073512989404.html/

59.online.wsj.com/article/SB10001424127887323777204578189391813881534.html/

60.online.wsj.com/article/SB10001424127887324784404578143144132736214.html/

61.online.wsj.com/article/SB10001424052748703294904575385532109190198.html/

62.online.wsj.com/article/SB10001424052748703940904575395073512989404.html/

63.*Ibid.*

64.*Ibid.*

65.*Ibid.*

66.*Ibid.*

67.online.wsj.com/article/SB10001424127887324784404578143144132736214.html/

68.http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-and-104-other-companies-are-tracking-me-on-the-web/253758/

69.http://archive.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213/

70.http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63/

71.http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213/

72.http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

73.http://arstechnica.com/tech-policy/2009/03/pulling-back-the-curtain-on-anonymous-twitterers/

74.http://www.onthemedia.org/2012/mar/02/end-anonymous-commenting/

75.http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

76.http://infotrope.net/2011/07/25/preliminary-results-of-my-survey-of-suspended-google-accounts/

77.http://www.guardian.co.uk/technology/2012/apr/19/online-identity-authenticity-anonymity/

78.http://www.zephoria.org/thoughts/archives/2010/01/16/facebooks_move.html/

79.http://www.livescience.com/6199-cyberbullying-rampant-lesbian-gay-teens.html/

80.http://www.numerama.com/magazine/23499-la-justice-sud-coreenne-juge-l-anonymat-indispensable-a-la-liberte-d-expression.html/

81.http://blogs.wsj.com/tech-europe/2013/01/17/the-debate-over-online-anonymity/

82.[de Marco, 2005]

83.[Cohen, 1996]

84.[Lessig, 2006]

85.[Weiss, 2010]

86.[Manach, 2010]

87.[Solove, 2011]

88.http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

89.http://www.nextinpact.com/news/75153-californie-loi-levant-anonymat-delinquants-bloquee-momentanement.htm/

90.Cité dans [Solove, 2011].

91.http://www.nytimes.com/2012/09/09/technology/data-driven-discovery-is-techs-new-wave-unboxed.html/

92.http://www.wired.co.uk/magazine/archive/2011/12/features/the-news-forecast/

93.http://www.mondaynote.com/2012/09/23/facebooks-gen-y-nightmare/

94.http://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf

95.http://www.slate.fr/life/86451/cacher-grossesse-internet-suspect-donnees

96.[Greenwald, 2014]

97.[de Marco, 2005]

98.http://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789/

99.http://fr.wikipedia.org/wiki/Article_8_de_la_Convention_européenne_des_droits_de_l'homme

100.[de Marco, 2005]

101. http://arstechnica.com/tech-policy/2012/12/op-ed-a-plea-to-google-protect-our-e-mail-privacy/

102. http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=CA5AD1ED1A4DDC0350D17617106ACF80.tpdjo16v_1?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417506

103. http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418646&cidTexte=LEGITEXT000006070719

104. http://techcrunch.com/2012/04/23/your-are-worth-4-84/

105. http://www.rue89.com/2012/02/15/iphone-vos-applications-font-joujou-avec-votre-carnet-dadresse-229423/

106. http://online.wsj.com/article/SB10001424052748703748904575411530096840958.html?mod=WSJ_WhatTheyKnow2010_RightTopBelowCarousel/

107. https://www.eff.org/deeplinks/2010/08/government-finds-uses-social-networking-sites/

108. http://www.washingtonpost.com/world/national-security/fbi-investigation-of-broadwell-reveals-bureaus-comprehensive-access-to-electronic-communications/2012/11/17/5f27d636-3012-11e2-9f50-0308e1e75445_story.html

109. http://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal/

110. [Chahid-Noura, 2001]

111. [Colin & Verdier, 2012]

112. http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/

113. http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html/

114. https://ssd.eff.org/risk/

115. https://ssd.eff.org/risk/lessons/

116. http://bluetouff.com/2010/10/05/anonymat-acte-1-vpn-et-hadopi-et-vous-vous-pensez-anonymes/

117. http://www.nextinpact.com/news/76432-navigateurs-parts-marche-relativement-stables-durant-2012.htm/

118. https://www.mozilla.org/en-US/firefox/all/

119. http://www.chromium.org/Home/chromium-privacy/
120. https://ssd.eff.org/tech/browsers/
121. *Ibid.*
122. [Eckersley, 2010]
123. http://howto.cnet.com/8301-11310_39-57368016-285/how-to-prevent-google-from-tracking-you/
124. http://owni.fr/2010/06/01/votre-historique-mis-a-nu/
125. http://support.mozilla.org/fr/kb/navigation-privee-naviguer-sans-conserver-infos-sites/
126. http://lifehacker.com/5861440/ghost-incognito-automates-your-private-browsing-in-chrome/
127. http://www.lemonde.fr/technologies/article/2010/08/07/la-navigation-privee-des-navigateurs-n-est-pas-fiable-a-100_1396474_651865.html
128. http://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-flash.html
129. http://www.lemonde.fr/technologies/article/2014/04/09/une-enorme-faille-de-securite-dans-de-nombreux-sites-internet_4397995_651865.html
130. http://www.clubic.com/navigateur-internet/actualite-515761-extension-https-everywhere-disponible-3.html/
131. http://www.lemonde.fr/technologies/article/2013/09/06/pour-casser-les-clefs-de-chiffrement-la-nsa-a-du-tricher_3472728_651865.html
132. http://arstechnica.com/tech-policy/2012/11/new-data-on-privacy-policies-shows-20-percent-of-sites-may-sell-data/
133. http://www.slate.com/blogs/future_tense/2012/12/18/instagram_privacy_uproar_why_it_s_absurd_in_three_nearly_identical_sentences.html/
134. http://www.nytimes.com/2012/05/03/technology/personaltech/how-to-muddy-your-tracks-on-the-internet.html
135. https://www.eff.org/who-has-your-back-government-data-requests-2014
136. http://www.theregister.co.uk/2012/08/30/wang_dissident_yahoo_free_from_prison/
137. http://www.guardian.co.uk/technology/2012/apr/22/me-and-my-data-internet-giants/
138. http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html/

139. http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/facebook-supprime-enfin-les-photos-supprimees-17-08-2012-1496835_506.php
140. http://www.guardian.co.uk/technology/2012/apr/22/me-and-my-data-internet-giants/
141. http://techcrunch.com/2013/01/01/the-one-charm-of-the-past-is-that-it-is-the-past/
142. [Rallet & Rochelandet]
143. *Ibid.*
144. *Ibid.*
145. [Georges, Sallantin & Seilles, 2010]
146. http://www.zephoria.org/thoughts/archives/2010/01/16/facebooks_move.html/
147. *Ibid.*
148. http://lifehacker.com/5843969/why-facebook-is-tracking-your-every-move-on-the-web-and-how-to-stop-it/
149. http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track/
150. http://bits.blogs.nytimes.com/2012/05/17/twitter-implements-do-not-track-privacy-option/
151. http://usatoday30.usatoday.com/tech/news/story/2011-12-29/internet-privacy/52274608/1/
152. *Ibid.*
153. http://www.ranum.com/security/computer_security/editorials/point-counterpoint/bigbrother.html
154. http://www.google.com/transparencyreport/saferemail/#region=150
155. http://ideas.time.com/2013/01/02/the-government-would-like-to-keep-reading-your-email/
156. http://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal/
157. http://www.pcinpact.com/news/70383-fbi-serveur-mixmaster-remailer-anonymat.htm/
158. http://www.wired.com/threatlevel/2012/04/fbi-seizes-server/
159. http://www.wired.com/threatlevel/2010/04/nsa-executive-charged/
160. http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/

161. http://rue89.nouvelobs.com/rue89-eco/2012/09/27/votre-patron-le-droit-de-lire-vos-e-mails-pros-et-persos-235649/
162. https://www.eff.org/deeplinks/2012/11/tutorial-how-create-anonymous-email-accounts/
163. http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistle-blower
164. http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html
165. http://googleonlinesecurity.blogspot.fr/2014/06/making-end-to-end-encryption-easier-to.html
166. http://owni.fr/2012/11/06/silent-circle-brouille-lecoute/
167. http://www.slate.com/articles/technology/future_tense/2012/10/silent_circle_mike_janke_s_iphone_app_makes_encryption_easy_governments.2.html/
168. http://web.jabber.ccc.de/?page_id=5/
169. https://crypto.cat/
170. http://www.slate.com/blogs/future_tense/2012/07/20/skype_won_t_comment_on_whether_it_can_now_eavesdrop_on_conversations_.html/
171. http://www.inria.fr/centre/sophia/actualites/comment-skyper-sans-etre-observe/
172. http://www.slate.com/blogs/future_tense/2012/07/20/skype_won_t_comment_on_whether_it_can_now_eavesdrop_on_conversations_.html/
173. http://www.nytimes.com/2012/12/01/world/middleeast/syrian-rebels-turn-to-skype-for-communications.html
174. http://www.guardian.co.uk/technology/2012/dec/14/china-tightens-great-firewall-internet-control/
175. https://www.usenix.org/legacy/event/leet11/tech/full_papers/LeBlond.pdf
176. [Greenberg, 2012]
177. http://www.lemonde.fr/technologies/article/2013/10/04/la-nsa-a-tente-de-casser-l-anonymat-du-reseau-tor_3490357_651865.html
178. http://www.forbes.com/forbes/2006/0227/090_2.html/
179. https://blog.torproject.org/blog/ultrasurf-definitive-review/
180. http://ultrasurf.us/Ultrasurf-response-to-Tor-definitive-review.html/

181. http://b.averysmallbird.com/entries/the-need-for-community-participation-and-clear-disclosure-processes-in-the-case-of-ultrasurf/
182. https://blog.torproject.org/blog/ultrasurf-definitive-review/
183. http://www.nytimes.com/2013/01/06/technology/legislation-would-regulate-tracking-of-cellphone-users.html
184. http://www.itworld.com/it-management/311197/those-free-apps-can-cost-you-big/
185. http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/
186. http://arstechnica.com/security/2012/08/passwords-under-assault/
187. http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/
188. http://www.wired.com/2014/04/tails
189. [Duhen, 2010]
190. https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment/
191. *Ibid.*
192. http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html?mod=djemalertTECH/
193. http://www.rue89.com/2012/06/06/proteger-nos-donnees-perso-sur-le-web-bon-courage-m-hollande-232558/
194. http://www.redressement-productif.gouv.fr/rapport-sur-fiscalite-secteur-numerique/
195. http://www.lemonde.fr/pixels/article/2014/05/31/premieres-demandes-a-l-oubli-adressees-a-google_4429680_4408996.html
196. http://www.rtl.fr/culture/web-high-tech/droit-a-l-oubli-numerique-google-a-recu-12-000-requetes-en-une-journee-7772354519
197. http://www.zdnet.fr/actualites/droit-a-l-oubli-bing-proposera-aussi-son-formulaire-39802383.htm
198. http://www.lemonde.fr/idees/article/2012/05/31/un-reseau-social-voue-a-la-disparition_1710612_3232.html
199. http://archives.fing.org/identitesactives.net/index.html%3Fq=accelerateur-de-projets-carte-identite-blanche.html
200. http://bugbrother.blog.lemonde.fr/2012/11/26/facebook-google-vecteurs-de-chienlit/
201. http://www.technologyreview.com/news/428045/the-curious-case-of-internet-privacy/

202. http://linuxfr.org/users/uld/journaux/commander-une-pizza-en-2015/
203. http://www.mondaynote.com/2012/09/23/facebooks-gen-y-nightmare/
204. [Benichou, 2001]
205. http://bugbrother.blog.lemonde.fr/2009/04/22/comment-contourner-la-cybersurveillance/
206. [Hirshleifer, 1980]
207. [Gavison, 1980]
208. http://owni.fr/revue-du-web/15-des-jeunes-suedois-se-cachent-en-ligne/
209. [Greenberg, 2012]
210. http://www.lemonde.fr/technologies/article/2012/10/02/bug-facebook-pas-de-messages-prives-mais-des-conversations-a-caractere-prive-selon-la-cnil_1768954_651865.html
211. http://www.technologyreview.com/news/428045/the-curious-case-of-internet-privacy/
212. http://fr.wikipedia.org/wiki/Commotion
213. http://bugbrother.blog.lemonde.fr/2012/11/26/facebook-google-vecteurs-de-chienlit/
214. http://fr.wikipedia.org/wiki/Jargon_informatique#C/
215. [Greenberg, 2012]
216. http://bluetouff.com/2010/10/05/anonymat-acte-1-vpn-et-hadopi-et-vous-vous-pensez-anonymes/
217. [Front Line & Tactical Technology Collective]
218. [Collectif, 2011]
219. http://www.framasoft.net/article4127.html
220. https://www.schneier.com/blog/archives/2011/10/fbi-sponsored_b.html
221. www.lemonde.fr/pixels/article/2014/06/04/l-etrange-disparition-du-logiciel-truecrypt_4431134_4408996.html
222. http://www.lemonde.fr/technologies/article/2014/04/09/une-enorme-faille-de-securite-dans-de-nombreux-sites-internet_4397995_651865.html
223. [Collectif, 2011]
224. https://www.eff.org/who-has-your-back-2014
225. http://www.youtube.com/watch?v=G_7IcuSJ1-k
226. http://fr.wikipedia.org/wiki/USA_PATRIOT_Act
227. http://www.theregister.co.uk/2011/09/26/hidemyass_lulzsec_controversy/

228. http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html/

229. *Ibid.*

# Bibliographie


[Benichou, 2001]
Benichou, M. (2001). « Le Résistible déclin du secret », *Les Petites Affiches*, nº 122.

[Bok, 1989]
Bok, S. (1989). *Secrets: On the Ethics of Concealment and Revelation*. Vintage.

[Brim & Ruebhausen, 1965]
Brim, G. O. et Ruebhausen, O. M. (1965). « Privacy and Behavioral Research », dans *Columbia Law Review*, vol. 65, nº 7.

[Chahid-Noura, 2001]
Chahid-Noura, N. (2001). *Secret et nouvelles technologies* [table ronde], sous la présidence de Benayoun-Nakache, Y. *Les Petites Affiches*, nº 122.

[Cohen, 1996]
Cohen, J. E. (1996). « A Right to Read Anonymously: A Closer Look at "Copyright Management" », dans C*yberspace. Georgetown Law Faculty Publications and Other Works*, vol. 814.
http://scholarship.law.georgetown.edu/facpub/814/

[Colin & Verdier, 2012]
Verdier, H. et Colin, N. (2012). *L'âge de la multitude : Entreprendre et gouverner après la révolution numérique*. Armand Colin.

[Collectif, 2011]
Collectif. (2011). *How to Bypass Internet Censorship* (2e édition). FLOSS Manuals.
Voir aussi la traduction française (*Comment contourner la censure sur Internet ?*) aux formats PDF, EPUB, HTML sur :
http://www.howtobypassinternetcensorship.org/fr.html/

[de Marco, 2005]
de Marco, E. (2005). *L'anonymat sur Internet et le droit* [thèse].

[Duhen, 2010]
Duhen, W. (2010). « FAI face à l'anonymat sur Internet : vers de nouvelles responsabilités », dans Vétois, J. (dir.), « Technologies et usages de l'anonymat sur Internet », *Terminal*, no 105. L'Harmattan.

[Eckersley, 2010]
Eckersley, P. (2010). *How Unique Is Your Web Browser?* Springer.

[Enguehard & Panico, 2010]
Enguehard, C. et Panico, R. (2010). « Technologies et usages de l'anonymat sur Internet » dans Vétois, J. (dir.), *Terminal*, no 105. L'Harmattan.

[Front Line & Tactical Technology Collective]
Security in-a-box : trousse de sécurité ; outils et tactiques de sécurité numérique est un site web créé par Front Line et Tactical Technology Collective qui comprend un livret et des guides pratiques autour de la sécurité sur Internet.
https://securityinabox.org/fr/

[Gavison, 1980]
Gavison, R. (1980). « Privacy and the Limits of Law », *Yale Law Journal*, vol. 89, no 3.

[Georges, Sallantin & Seilles, 2010]
Georges, F., Sallantin, J. et Seilles, A. (2010). « Des illusions de l'anonymat : les stratégies de préservation des données personnelles à l'épreuve du Web 2.0 », dans Vétois, J. (dir.), « Technologies et usages de l'anonymat sur Internet », *Terminal*, no 105. L'Harmattan.

[Greenberg, 2012]
Greenberg, A. (2012). *This Machine Kills Secrets: How Wikileakers, Hacktivists, and Cipherpunks Are Freeing the World's Information*. Ebury Press.

[Greenwald, 2014]
Greenwald, G. (2014). *Nulle part où se cacher*. JC Lattés.

[Hirshleifer, 1980]
Hirshleifer, J. (1980). « Privacy: Its origin, Function, and Future », *Journal of Legal Studies*, vol. 9.

[Lecomte, 2010]
Lecomte, R. (2010). « L'anonymat comme "art de résistance" : le cas du cyberespace tunisien », dans Vétois, J. (dir.), « Technologies et usages de l'anonymat sur Internet », *Terminal*, nº 105. L'Harmattan.

[Lessig, 2006]
Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

[Manach, 2010]
Manach, J-M. (2010). *La vie privée, un problème de vieux cons ?* FYP éditions.

[Merzeau, 2009]
Merzeau, L. (2009). « Présence numérique : les médiations de l'identité », dans *Les Enjeux de l'information et de la communication* (revue en ligne du Gresec).
http://w3.u-grenoble3.fr/les_enjeux/2009/Merzeau/Merzeau.pdf/

[Rallet & Rochelandet, 2010]
Rallet, A. et Rochelandet, F. (2010). « Exposition de soi et décloisonnement des espaces privés : les frontières de la vie privée à l'heure du Web relationnel », dans Vétois, J. (dir.), « Technologies et usages de l'anonymat sur Internet », *Terminal*, nº 105. L'Harmattan.

[Rochelandet, 2010]
Rochelandet, F. (2010). *Économie des données personnelles et de la vie privée*. La Découverte.

[Solove, 2011]
Solove, D. (2011). *Nothing to Hide. The False Tradeoff Between Privacy and Security*. Yale University Press.

[Weiss, 2010]
Weiss, M-A. (2010). « Est-il légal de demeurer anonyme sur Internet selon le droit des États-Unis ? », dans Vétois, J. (dir.), « Technologies et usages de l'anonymat sur Internet », *Terminal*, nº 105. L'Harmattan.

# Index


## A

ACTA 13
actifs (assets) 54
Adblock Plus 96
adresse IP 76, 205
adversaire 54
AIM 133
anonymat
    cinq commandements 56
    définition 1
    neutralité 3
    partiel 3
    relatif 2
Anonymous 211
anti-tracking 99
assets 54
asymétrie de l'information 48

## B

backdoor 208
Big Brother 23
Boyd, Danah 5, 35, 93, 94
Broadwell, Paula 211

## C

carte d'identité blanche électronique 191
Chahid-Noura, Noël 49
chaise-clavier (interface) 202
chat 132
chiffrement 116, 131
    asymétrique 119
    symétrique 119
Chrome 64, 66
Chromium 65
Circumventor 186
CISPA 13
clef
    génération 121, 125
    privée 120
    publique 120
    serveur 127
    stockage 128
Code 18 202
Code 45 202
Code des postes et des communications électroniques 183
Code pénal 45
Cohen, Julie E. 37
cohérence 55
collecte de données 80
Commotion (réseau) 199
conditions générales d'utilisation 82
confidentialité 54, 117
Conseil constitutionnel 44
consistency 55
Constitution américaine 37
contrôle 55
Corée du Sud 36
cryptographie 116
cryptopartie 187

## D

DADVSI 13
Dashlane 181
de Marco, Estelle 36
Déclaration des droits de l'homme de 1789 44
Didn't Read 83
Dingledine, Roger 206
Discretio 171
disponibilité 55
DMCA 13
DNS 77
Do Not Track 67, 98, 190
Doctorow, Cory 192
donnée
  anonymisée 26, 27
  de connexion 14
Drake, Thomas 204
Droidwall 170
droit à l'anonymat 46

## E

e-commerçant 17, 18
Electronic Frontier Foundation 66, 73, 188, 210
e-mail 103
  anonyme 114
  client 104
  en-tête 106
  jetable 114
  serveur 104
  vulnérabilité 105
empreinte 122
Enigmail 124
entraînement 213
erreur humaine 213
European Privacy and Human Rights 49

## F

Facebook 21, 22, 36, 91, 94
Firefox 64, 65
fournisseur d'accès à Internet (FAI) 182, 183
  fédération FDN 183
fournisseur de mail 108
Freenet 164
Frontline Defenders 188

## G

Gmail 88, 109
GnuPG 119
Google 87, 91
  Dashboard 87
Google+ 21, 34
Guardian Project 173

## H

habeas corpus numérique 190
Hadopi 13
harcèlement 35
historique de navigation 68
HTTP 75
HTTPS everywhere 72
Hushmail 110
hypermnésie XIX

## I

ICQ 133
identification 28
identité 97
IMAP 104
infrastructure décentralisée 209
Instagram 91
intégrité 54, 117
IRC 133

## J

Jabber 133
jailbreaker 175
JAP 165
Jarvis, Jeff 8
JavaScript 76

## K

keylogger 141
Korben 187

## L

LCEN 13
Lessig, Lawrence 14, 34, 37, 192
Lewman, Andrew 34
Liberation Tech 188
liberté d'expression 36
little brothers 23
logiciel libre 208
logs 14
loi Informatique et libertés 45
LOPPSI 2 13
Lyons, Daniel 21

## M

menace 54
  défaillance 50
  entreprise 47
  État 49
  piratage 50
  police 49
  proche 51
Merzeau, Louise 23, 47
MesInfos 191
messagerie instantanée 132
  OTR 135
Midata 191
Minitel 18
modèle économique 19, 21
mot de passe 180
  commandements 178
  stocker 180
  vulnérabilité 177
moteur de recherche 87

## N

navigateur 62, 64, 71
  cookie 71
  mode privé 69
  protection 65
  trace 67, 77
navigation 62, 173
  privée 69
New Yorker 11
non-répudiation 117

## O

Ohm, Paul 30
OpenPGP 118, 129
Opéra 64
opt-out 22, 96
ordinateur professionnel 113
OTR 135

## P

Passpack 180
Patriot Act 211
Petraeus, David 211
PGP 118
phrase de passe 121
PIPA 13
pirate box 199
pistage 94
Piwik 182
POP 104
porte dérobée 208
possibilité d'audit 55
Privacy Bill of Rights 190

Privacy Enhancing Technologies (PET) 188
privacy policies 82
Privacy rights 50
protocole de courriel 104
proxy 143
    CGIProxy 186
    extension 149
    HTTP 146
    SOCKS 146
    utilisation 147
    web 146
pseudonymat 9, 35
Psiphon 165
publicitaire 96

## R

Reddit 188
RedPhone 171
Reporters Sans Frontières 188
réseau social 49, 92, 94
Riseup 110
risque 54, 202
    vs menace 55
rooter 175

## S

Safari 64
Schmidt, Eric 211
Security in-a-box 187
signature 122
Silent Circle 173
site marchand 17
Skype 133, 139
smartphone
    faiblesse 168
SMS
    chiffrer 171
Soljénistyne, Alexandre 39
Solove, Daniel J. 37, 39
suicide machine 90
surveillance 24
système d'exploitation orienté sécurité 181
    AnonymOS 181
    Knoppix 181
Syverson, Paul 206

## T

Tactical Tech 188
Tails 181
technologie prédictive 41
terms of service 82, 83
texto
    chiffrer 171
TextSecure 172
Tor 159, 184, 206
    aider 184
    fonctionnement 160
    Lewman, Andrew 34
    nœud de sortie 185
    pair à pair 163
    Vidalia 184
trace 8, 80
    involontaire 81
    volontaire 81
tracker 23, 96
tracking 48
Turow, Joe 26
Twitter 91, 95

## U

Ultrasurf 165
user agent 77

## V

Vidalia 184
vie privée 8, 44

autonomie 4
contrôle 5
définition 3
Montaigne 3
quiétude 4
secret 4
vie publique 7
VoIP 139
voix sur IP 139
VPN 150, 174
Anonine 159
avantage 159
Chine 152
choix 155
compatibilité 158
configuration 153
Hidemyass 211
inconvénient 151
Ipredator 159
moyen de paiement 158
Mullvad 159
no log 152, 157
OpenVPN 153, 157
PPTP 153, 157
protocole 157
référence 159
ressource 154
siège social 156
vitesse de connexion 158

## W

webmail 104, 108
alternatif 109
commercial 108
whistleblowers 196
Wickr 173
Windows Live Messenger 133

## X

XMPP 133

## Y

YouTube 88

## Z

Zimmerman, Philip 118