Framatophe

Libertés numériques

Guide de bonnes pratiques à l'usage des DuMo

Mise à jour : novembre 2017

Framasoft est un réseau d'éducation populaire, issu du monde éducatif, consacré principalement au logiciel libre. Il s'organise en trois axes sur un mode collaboratif : promotion, diffusion et développement de logiciels libres, enrichissement de la culture libre et offre de services libres en ligne.

Pour plus d'informations sur Framasoft, consultez `http://www.framasoft.org`.

Se démarquant de l'édition classique, les Framabooks sont dits « livres libres » parce qu'ils sont placés sous une licence qui permet au lecteur de disposer des mêmes libertés qu'un utilisateur de logiciels libres. Les Framabooks s'inscrivent dans cette culture des biens communs qui favorise la création, le partage, la diffusion et l'appropriation collective de la connaissance.

Pour plus d'informations sur le projet Framabook, consultez `http://framabook.org`.

ISBN : 979-10-92674-15-6
Prix : 8 euros
Dépôt légal : 2017, lulu.com
Mise en page avec Pandoc et LaTeX
Couverture : dessins tirés de l'œuvre de Simon « Gee » Giraudot, sous Creative Commons By-Sa.

Vous pouvez encourager l'auteur par un don sur
fr.liberapay.com/Framatophe

Remerciements

Je tiens ici à remercier toutes celles et ceux sans qui ce petit guide n'aurait pas vu le jour. Ils m'ont aussi donné l'opportunité d'acquérir les quelques connaissances qui me permettent de passer pour le spécialiste que je ne suis pas.

— Ma chère épouse, relectrice avisée, patiente et compréhensive…
— Mon cher Goofy, pour sa relecture attentive…
— Mes chers amis de Framasoft…
— Toute la communauté libriste francophone et quelques correspondants avisés, tels Thelvaën Mandel, fmr, Tuxman…
— Libre Fan pour sa relecture de la version de novembre 2017.

Introduction

Trop compliqué ! pas l'temps… ultra-sollicités entre nos communications, nos applications et nos appareils nous n'avons paradoxalement guère le temps de nous interroger sur la pertinence de nos besoins logiciels, leurs configurations, la sécurité de nos données et, au-delà, sur nos pratiques numériques.

Mais qui prend ce temps aujourd'hui ? Nous devons tous plus ou moins faire confiance aux éditeurs de logiciels. Tout se passe comme si la réflexion sur les usages était la prérogative des passionnés d'informatiques, ces hackers venus d'un monde alternatif, ces voisins bienveillants chez qui tout le monde vient chercher la solution à ses petits ennuis d'ordinateur.

Dans ce monde, jusqu'à une époque récente, les discussions allaient bon train, reprenant bien souvent avec moquerie les mésaventures logicielles de Madame Michu. Or, lassée des réflexions machistes dont elle faisait l'objet, Françoise Michu a pris sa retraite bien méritée. C'est désormais la famille Dupuis-Morizeau (qu'on abrégera en DuMo) qui se porte volontaire pour supporter ces geeks qui prétendent penser à la place des autres. Bien plus informés que Madame Michu, habitués des environnements informatiques en tout genre, les DuMo assumeront ce nouveau rôle dans

un domaine où les caricatures sont nombreuses, entre la « génération Y », la secrétaire perdue, et les grands-pères ultra-connectés.

Qui sont les DuMo ? une famille avec un pouvoir d'achat moyen (mais solide), récemment abonnée à la fibre dans leur petit pavillon d'un village normand [1]. Les comptes de messagerie des membres de la famille sont chez Google, gérés de main de maître par le grand fils, lycéen, dont le profil Facebook possède plus de 100 followers, une fierté. La petite, elle, vient de passer au collège le Brevet Informatique et Internet aux normes européennes Digcomp [2], et sait parfaitement maîtriser toute la suite bureautique de Microsoft. Madame, elle, a suivi consciencieusement les formations qui lui étaient offertes sur Powerpoint et envoie régulièrement à ses contacts de magnifiques diaporamas avec des couchers de soleil mauves. Quant à Monsieur, il maintient un blog, gère les comptes bancaires en ligne, mais se plaint souvent de la lenteur de l'ordinateur familial et songe sérieusement à en acheter un nouveau.

Caricature ? Oui… mais pas parce que les DuMo sont des consommateurs de services. Le problème, les DuMo le connaissent et en sont parfaitement conscients : leur méconnaissance d'Internet, l'opacité à leurs yeux des mécanismes à l'œuvre sur les serveurs que fréquentent leurs machines (ordinateur, smartphones et tablette) lorsqu'ils utilisent des services web, leurs difficultés à remédier aux « pannes » qu'ils rencontrent régulièrement, les limites de leurs savoirs-faire lorsqu'il faut utiliser des logiciels pour opérer quelques opérations plus complexes que d'habitude, les abandons frustrants devant l'apparente complexité de la configuration de leur système d'exploitation ou des logiciels de messagerie… tout cela leur fait sérieusement douter de leur autonomie numérique.

Jamais Internet n'a été autant source d'inquiétudes et de tensions. On ne compte plus les ouvrages sur le loup (ou l'ogre)

1. La famille DuMo est un levier scénaristique. Elle *n'existe pas*, ni en réalité (ou alors toute ressemblance serait vraiment fortuite…), ni même en théorie, car on se doute bien que dans ces conditions qui respirent la guimauve et l'ennui, les choses pourraient vite mal tourner, entre l'alcool, la drogue et le sexe, au grand bénéfice de la presse à sensation.

2. `https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework`

Google, sur les « dangers d'Internet », sur les risques liés à la confidentialité des données personnelles, sur la surveillance numérique des individus, sur la surveillance globale des populations… Tout cela est à la fois anxiogène et, en même temps, très peu d'ouvrages proposent des solutions concrètes [3], accessibles à tous et facilement, pour affronter ce monde plein d'embûches.

Mais comment comprendre ces enjeux si, d'un autre côté, les outils et les composants de l'environnement numérique restent des boîtes noires ? L'utilisation de logiciels libres, ceux que l'on peut partager et que la communauté peut expertiser et améliorer, est un premier pas vers l'autonomie numérique, une approche raisonnée et sereine de l'informatique et des réseaux. Or les logiciels ne font pas tout. Les pratiques des utilisateurs, en connaissance de cause, sont les éléments centraux d'un autre monde numérique, moins anxiogène et plus durable, éthique et solidaire.

Cet ouvrage s'adresse donc aux DuMo. Il est à la fois un manuel et un livre de conseils pratiques. L'objectif est de permettre au lecteur de différencier les bonnes pratiques de celles qui ne sont pas adaptées à ses besoins (et faussent ses apprentissages en matière de logiciels) ou mettent en danger son intimité numérique (par exemple dans le domaine de la sécurité ou de l'usage des services web). Certaines sections pourront parfois paraître basiques, elles recèlent toujours une parcelle méconnue du sujet traité. Chaque chapitre considère un pilier des activités numériques, il en dessine les contours, soulève les enjeux et propose des solutions de logiciels libres dont la légitimité s'impose d'elle-même. Il est temps en effet, de formaliser quelques pratiques d'auto-défense numérique tout en permettant aux utilisateurs de s'approprier ces usages et ces outils, même s'ils ne sont pas libristes ou d'irréductibles activistes des libertés numériques.

Le deviendront-ils ? Ce n'est pas important. L'essentiel est qu'en essaimant les bonnes pratiques et les solutions logicielles alternatives, c'est vers un modèle d'environnement numérique serein et plus démocratique que nous nous dirigeons. C'est pourquoi

3. Il y en a au moins un, écrit par Tristan Nitot, *Surveillance :// Les libertés au défi du numérique : comprendre et agir*, C&F Éditions, Caen, 2016.

ce livre a aussi une ambition d'éducation populaire : il est placé sous licence libre, ce qui permet, dans le respect du droit d'auteur, de se l'approprier, de le modifier et de redistribuer des versions modifiées, enrichies de l'expérience et/ou à destination d'autres lecteurs. Emparez vous-en !

CHAPITRE 1

De quels outils ai-je besoin ?

Comme dans bien des domaines, les techniques supposent des apprentissages. Ainsi, lorsque vous avez acheté votre ordinateur, et comme il y a de fortes chances qu'il ait été équipé d'emblée d'un système d'exploitation, vous avez dû apprendre à vous en servir pour répondre à vos besoins du moment : relier l'ordinateur à votre box Internet, ouvrir le navigateur, faire les premières mises à jour…

Le problème rencontré par beaucoup d'utilisateurs en matière de logiciel est de savoir identifier de quoi ils ont besoin. Dans beaucoup de cas, freinés par le prix de certains logiciels ou par simple méconnaissance de la diversité, les utilisateurs se rabattent naturellement vers des utilisations non adaptées : essayer d'ouvrir des photos dans un logiciel de traitement de texte, être dans l'impossibilité de lire des formats vidéos et être obligé de renoncer, devoir payer un logiciel dont on utilise la version d'essai pré-installée sur une nouvelle machine, etc. Tant de situations très courantes amènent les utilisateurs à se décourager ou ressentir de grandes

frustrations devant l'apparente complexité de l'informatique domestique.

Dans ce chapitre nous allons voir que les logiciels libres ne sont pas seulement des alternatives aux « grands » logiciels connus que « tout le monde utilise » : ils représentent autant de solutions diverses et sereines pour se servir d'un ordinateur de manière efficace. Nous pousserons alors un peu plus loin les cas d'usages pour parler des systèmes d'exploitation, des formats et des protocoles de communications.

1.1 Les logiciels libres : s'y retrouver

D'un point de vue néophyte, les logiciels libres sont souvent assimilés à des logiciels gratuits, disponibles sur Internet et téléchargeables. Même si le terme « gratuit » n'est pas adapté, ce n'est pas une si mauvaise opinion : les logiciels libres sont très nombreux et sont autant de solutions pour accomplir des tâches même similaires, sans avoir obligatoirement à débourser de l'argent.

Ainsi, le premier avantage de l'offre en logiciel libre, c'est la diversité. Cette dernière s'oppose à l'idée d'un quelconque monopole sur un secteur d'application donné. Pour donner un exemple simple : en 2008-2009, pour satisfaire aux exigences de la Commission Européenne sur la libre concurrence, Microsoft a mis en place un écran de choix de navigateurs Internet pour ne pas imposer l'utilisation d'Internet Explorer. Les utilisateurs peuvent alors choisir le navigateur Mozilla Firefox, qui est un logiciel libre, et l'utiliser par défaut.

Comment s'y retrouver dans cette offre ? Ce n'est pas évident. D'une part vous devez trouver le logiciel qu'il vous faut et d'autre part cela suppose de devoir identifier votre besoin de manière à affiner la recherche et trouver le bon logiciel.

Pour vous y aider, il existe au moins trois ressources :

1. Framalibre[1] est le projet historique d'annuaire de logiciel libre par Framasoft étendu à toutes les ressources libres (car il n'y a pas que les logiciels qui peuvent être libres). Dans cet annuaire, entretenu et augmenté par la communauté, vous pouvez entrer des mots-clés et afficher des alternatives pertinentes et des suggestions ;
2. Clibre[2] est un autre annuaire de logiciels libres avec un panel choisi ;
3. Une page Wikipédia « liste de logiciels libres[3] » vous permet aussi de trouver des logiciels, classés par catégories d'activités.

Un point commun important entre ces annuaires est qu'ils vous renvoient systématiquement vers les sites officiels des logiciels en question. C'est crucial : si vous devez télécharger un logiciel pour l'installer sur votre machine, faites-le toujours depuis le site officiel (ou depuis les dépôts officiels de votre distribution GNU/Linux si vous êtes dans ce cas). D'une part vous êtes sûr d'obtenir la dernière version, et d'autre part vous diminuez le risque d'installer une version modifiée (et non validée) qui pourrait causer des dommages sur votre machine ou, pire, la pirater.

Une autre précaution à prendre est de vous assurer de la licence du logiciel que vous comptez utiliser. Comme nous allons le voir, la gratuité n'est pas l'apanage du logiciel libre et tous les logiciels gratuits ne sont pas dotés des meilleures intentions. Fiez-vous donc de préférence aux annuaires mentionnés ci-dessus.

1.2 Les logiciels libres : qu'est-ce ?

Une fois que vous avez installé un ou plusieurs logiciels libres et que vous commencez à les éprouver, il est temps de prendre un

1. `https://framalibre.org`
2. `http://www.clibre.eu/`
3. `https://fr.wikipedia.org/wiki/Liste_de_logiciels_libres`

petit peu de recul sur ce qu'implique le caractère *libre* du logiciel libre.

Le mouvement du logiciel libre est né au début des années 1980, en réaction à une transformation de l'économie du logiciel. Auparavant, les programmes étaient fournis avec les machines de manière gratuite et ouverte afin de faciliter et optimiser l'emploi de ces machines. La communauté des programmeurs pouvait alors s'échanger ces programmes, les modifier et les adapter aux besoins… jusqu'au moment où certaines firmes en décidèrent autrement pour s'approprier l'innovation des logiciels et maîtriser les usages. Sous l'impulsion de Richard M. Stallman, un programmeur qui a assisté à cette transformation, le mouvement du logiciel libre est né avec l'idée qu'un programme doit demeurer accessible, ouvert, modifiable et diffusable. Richard M. Stallman fonda alors le projet GNU [4] et, avec des amis, la Free Software Foundation [5], aujourd'hui de renommée mondiale, qui a pour but de promouvoir et défendre le logiciel libre. Le projet GNU permit de mettre au point la Licence Publique Générale (GNU GPL), d'un point de vue juridique, qui définit le logiciel libre et les conditions d'usage du logiciel placé sous cette licence.

Les quatre libertés du logiciel libre

1. la liberté d'exécuter le programme, pour tous les usages,
2. la liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins,
3. la liberté de redistribuer des copies du programme,
4. la liberté d'améliorer le programme et de distribuer ces améliorations au public, pour en faire profiter toute la communauté.

(Voir la page Wikipédia consacrée au « Logiciel Libre [a] ».)

a. `https://fr.wikipedia.org/wiki/Logiciel_libre`

4. `https://www.gnu.org/gnu/thegnuproject.fr.html`
5. `https://www.fsf.org/?set_language=fr`

Les libertés du logiciel libre impliquent :

— que le logiciel est disponible de manière égalitaire et sans restriction,
— que le logiciel est auditable par la communauté (il ne peut contenir de code malveillant ou si c'est le cas, très rapidement décelé),
— que le fonctionnement du logiciel est ouvert et permet d'innover sur cette base,
— que l'on peut donner des copies du logiciel, ou les vendre (ne serait-ce que pour couvrir les frais de main-d'œuvre),
— que l'on peut redistribuer le logiciel, y compris sous une version modifiée,
— que les modifications peuvent être elles aussi distribuées à toute la communauté.

Du point de vue individuel, que l'on contribue ou non au logiciel libre, le fait d'en utiliser implique :

— une limitation des risques de sécurité,
— une qualité dans les attentes concrètes du logiciel : il fera ce pourquoi il a été conçu,
— un suivi dans les améliorations du logiciel, à l'écoute de ses utilisateurs (même sans être programmeur vous pouvez faire part de vos remarques et difficultés et contribuer ainsi au développement),
— la possibilité de donner à vos proches une copie du logiciel ou les encourager à l'installer, sans contrainte.

Vous comprenez maintenant pourquoi les logiciels libres sont la plupart du temps gratuits et, s'ils sont payants, c'est parce qu'on y ajoute du service ou de l'expertise, ce qui fait d'ailleurs vivre beaucoup d'entreprises. Rien ne vous empêche, par ailleurs, d'encourager les développeurs en faisant des dons (bien souvent il existe près de chez vous des organisations à but non lucratif qui œuvrent pour le logiciel libre).

Activité	Logiciels non-libres	Logiciels libres
Traitement de texte	Microsoft Word	LibreOffice Writer, Abiword
Tableur	Microsoft Excel	LibreOffice Calc
Diaporama	Microsoft Powerpoint	LibreOffice Impress, Sozi
Gestion de courriel	Microsoft Outlook	Mozilla Thunderbird, Claws Mail
Dessin, retouche photos	Adobe Photoshop	Gimp
Graphisme, PAO	Adobe Indesign	Inkscape, Scribus
Lecture de documents PDF	Adobe Acrobat	Evince, Sumatra PDF
Navigation Internet	Microsoft Internet Explorer	Mozilla Firefox
Messagerie instantanée, voix, vidéo-chat	(Microsoft) Skype	Pidgin, Jitsi
Vidéo	Microsoft Windows Media Player	VLC, SMPlayer
Audio	Microsoft Windows Media Player	Amarok, VLC, Audacity

TABLEAU 1.1 – Quelques correspondances entre logiciels propriétaires et logiciels libres

1.3 Mes logiciels au quotidien

Dans un cadre domestique, les activités sur un ordinateur ne sont pas si nombreuses. Nous pouvons dresser un tableau des besoins les plus courants en identifiant de manière non exhaustive des logiciels libres adaptés aux différents exercices. Dans le tableau 1.1, nous listons des logiciels compatibles Windows.

Vous remarquerez, dans ce tableau, que seules deux firmes apparaissent dans les logiciels non-libres… Par exemple, pour « mieux » intégrer ses logiciels avec le système d'exploitation, Microsoft a choisi de développer de multiples secteurs d'application. Nous n'en avons ici qu'un petit aperçu. Du côté des logiciels libres, de multiples acteurs produisent des alternatives, ce qui fait que le choix ne se fait pas seulement entre logiciels libres et logiciels non-libres, mais aussi en fonction des approches différentes d'un même

besoin. Multiplier ces approches vous permettra de vous servir de ces logiciels libres de manière efficace, en choisissant d'utiliser à chaque fois le plus approprié.

1.4 Focus sur la suite LibreOffice

Une suite bureautique est un ensemble intégré de logiciels permettant d'accomplir un ensemble de tâches liées à la production de documents bureautiques. La suite LibreOffice [6] est la suite bureautique célèbre qui regroupe les applications suivantes :

— LibreOffice Writer : un logiciel de traitement de texte,
— LibreOffice Calc : un tableur,
— LibreOffice Impress : un créateur de diaporamas,
— LibreOffice Draw : pour la création de graphismes, schémas, diagrammes…
— LibreOffice Maths : un éditeur de formules mathématiques.

Bon à savoir

Une des originalités de LibreOffice est de proposer un dépôt officiel d'extensions [a] et de modèles [b] en tous genres. Vous y trouverez certainement ce que vous cherchez, entre fonctionnalités supplémentaires, packs d'icônes, modèles prêts à l'emploi…

a. `https://extensions.libreoffice.org/`
b. `https://extensions.libreoffice.org/templates/`

L'interface de LibreOffice est assez classique et ressemble à celle de Microsoft Office. Pour une première utilisation, prenez le temps de faire quelques essais puis reportez-vous à la documentation sur le Wiki de la Document Foundation [7] (éditeur de Libreoffice). Vous y trouverez des manuels, des tutoriels, des vidéos, autant de contenus que la communauté et la Document Foundation mettent à disposition des utilisateurs finaux.

6. `https://fr.libreoffice.org/`
7. `https://wiki.documentfoundation.org/Documentation/fr`

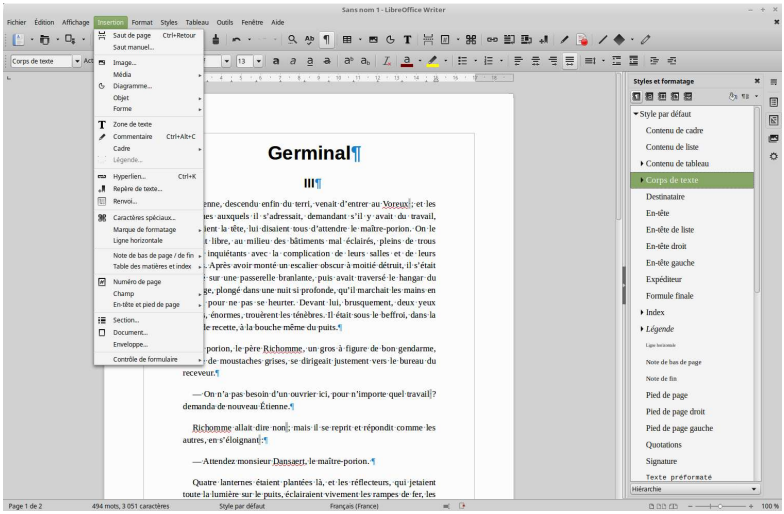


FIGURE 1.1 – LibreOffice Writer sous GNU/Linux Mint

Un fichier produit avec LibreOffice portera une extension par défaut selon le logiciel avec lequel vous l'avez créé : `.odt` pour Writer, `.ods` pour Calc, `.odp` pour Impress, `.odg` pour Draw. Néanmoins, LibreOffice peut lire et enregistrer des fichiers dans de multiples formats, notamment les formats de la suite Microsoft `docx`, `.xlsx`, `.doc`, `.xls`, ou même `.rtf`, `.pdf`, etc. Ainsi le passage ou la transmission de documents d'une suite à l'autre se fait généralement sans problème pour un usage courant[8].

Enfin, notez que des dictionnaires sont téléchargeables depuis le site officiel pour vous permettre d'utiliser le correcteur orthographique. Le projet Grammalecte[9] est plus abouti et intègre aussi de la correction grammaticale. Il permet aussi la correction typographique.

8. Si, par exemple, vos tableaux contiennent des macros spécifiques, la prudence est de mise.

9. `http://www.dicollecte.org/grammalecte/`

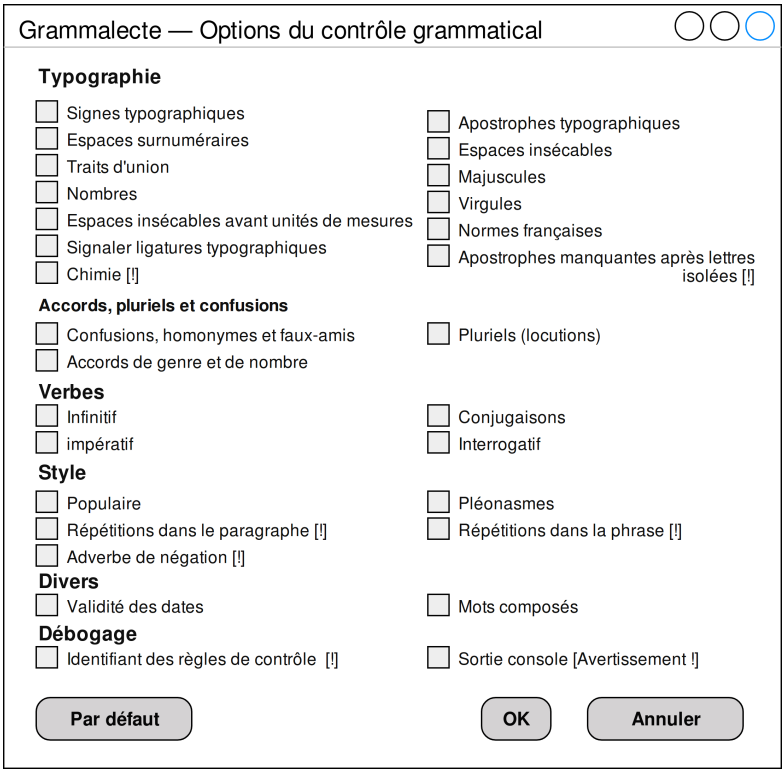


FIGURE 1.2 – Les options dans Gramalecte

1.5 Je peux aussi essayer des logiciels libres

Si l'installation de logiciels libres (ou l'installation d'une distribution GNU/Linux — cf. la fin de ce chapitre) vous intimide, il existe une solution facile : essayer des logiciels libres avec la Framakey [10]. Framakey est un projet de Framasoft consistant à rassembler sur une clé USB un ensemble de logiciels libres, intégrés en un système permettant de créer un bureau portable. En clair : vous disposez de vos logiciels sur une clé USB, vous pouvez la brancher sur n'importe quel ordinateur et utiliser ce bureau nomade, tout en enregistrant dessus (les données sont sauvegardées sur la clé). Très pratique, non ?

FIGURE 1.3 – Interface de la Framakey sous Windows

Il existe plusieurs versions de la Framakey dont trois sont des distributions GNU/Linux *live* : Linux Mint, Salix et Ubuntu. Vous pouvez utiliser ce bureau nomade directement en branchant votre clé alors que votre actuel système d'exploitation est en route : vous

10. `https://framakey.org/Pack/Framakey-Mint`

obtenez alors une interface dans un bureau « virtuel » et vous pouvez utiliser les logiciels libres proposés. Ou bien vous *bootez* sur la clé, vous pouvez utiliser la distribution GNU/Linux et même l'installer de manière permanente sur votre machine.

Vous pouvez aussi acheter cette Framakey [11], proposée par l'association Framasoft à la vente, et ne pas avoir à effectuer les manipulations de création de la clé. Une autre solution est de vous rendre à un événement libriste (répertorié sur l'Agenda du Libre [12]) : sur les stands, il est souvent possible de demander des clés similaires proposées comme *goodies* par les associations présentes (l'achat vous permet aussi de soutenir ces associations).

1.6 Les formats et l'interopérabilité

Lorsque vous échangez des documents, des photos ou n'importe quel fichier, quel que soit le logiciel qui vous a servi à les produire, vous devez vous assurer d'une chose au moins : que votre correspondant soit en mesure de les utiliser. C'est un des principes élémentaires de partage et de circulation de l'information : l'interopérabilité des formats.

Un format de fichier est une convention qui représente la manière dont sont arrangées et stockées les données regroupées dans ce fichier (et une donnée est un ensemble de *bits*, c'est-à-dire des 0 et des 1). Ces conventions permettent d'échanger les fichiers. Pour les lire, les programmes sont donc censés adopter ces conventions.

L'interopérabilité est la propriété d'un format de pouvoir être lu par plusieurs programmes différents ; c'est aussi un principe qui considère qu'un format de fichier ne doit pas être réservé à un programme en particulier. En effet, si l'éditeur d'un logiciel conçoit un programme capable de lire et d'enregistrer des fichiers uniquement lisibles par ce programme, les utilisateurs sont condamnés à l'utiliser exclusivement. Si l'éditeur ferme ses portes ou change les formats sans assurer la maintenance des formats qu'il utilise

11. `https://enventelibre.org/47-cles-usb`
12. `https://www.agendadulibre.org/`

à plusieurs années d'intervalles, vos fichiers deviennent inutilisables. C'est un peu comme si vous achetiez une voiture à essence avec l'obligation de vous rendre dans des stations-services d'une marque en particulier pour acheter la seule essence compatible.

Un bon format interopérable est censé être aussi ouvert et, mieux, libre : c'est-à-dire que ses spécifications techniques sont documentées et connues de tout le monde de manière à ce que les programmeurs puissent concevoir des logiciels capables de produire et lire des fichiers dans un format devenu de fait un *standard*. Par exemple, le format Open Document (ODF, Open Document Format) connu pour être produit par les logiciels de la suite LibreOffice (mais pas uniquement), est devenu en 2006 une norme ISO. Ce qui est loin d'être le cas pour d'autres formats pourtant bien connus comme le `.doc` dont Microsoft a par ailleurs cessé le développement au profit de OpenXML.

Ouvert ne signifie pas libre

Certains formats ouverts ne sont pas pour autant libres. Un format ouvert peut très bien devenir fermé. Un format libre est soumis à une licence libre (voir le chapitre 2), ce qui permet de verser les spécifications dans les biens communs (si son développement s'arrête, il pourra être repris par d'autres).

Enfin, le format Open Document étant une norme ISO, il est naturellement encouragé dans tous les pays de l'Union Européenne, cette dernière ayant publié plusieurs recommandations [13] pour son adoption dans les administrations publiques. En France, le Référentiel Général d'Interopérabilité [14] décrit les normes et les pratiques de l'administration publique. La version 2.0 du Référentiel a été adoptée officiellement en 2016 [15], et fait du format ODF la seule

13. `http://ec.europa.eu/idabc/en/document/3439/5887.html`
14. `http://www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/le-referentiel-general-interoperabilite-fait-peau-neuve`
15. `https://www.legifrance.gouv.fr/eli/arrete/2016/4/20/PRMJ1526716A/jo/texte`

norme recommandée dans les administrations publiques. Hélas, beaucoup d'entre elles sont encore prisonnières [16] des formats de la suite de Microsoft...

1.6.1 Bureautique

Dans le domaine de la bureautique, l'échange de fichiers donne lieu bien souvent à des contrariétés : recevoir un fichier et ne pas pouvoir l'ouvrir (ou bien en affichant des suites de caractères abscons), découvrir que votre diaporama est illisible sur l'ordinateur dédié à la vidéo-projection, s'apercevoir que la mise en page du document n'est plus valable d'une version d'un logiciel à l'autre, etc. Bien qu'à notre connaissance aucune étude n'ait vraiment été réalisée à ce sujet, toutes ces difficultés liées à l'utilisation des formats de fichiers fait perdre énormément de temps à tout le monde.

1.6.1.1 Enregistrer dans le bon format

Lorsque vous rédigez un document, avec un traitement de texte ou un tableur, vous avez tout intérêt à choisir un logiciel qui vous laissera le choix des formats d'enregistrement. C'est le cas de LibreOffice qui, au moment d'enregistrer un document, en utilisant la fonction `Fichier > Enregistrer sous...`, vous propose un grand choix de formats, normalisés ou non.

Il vous appartient d'enregistrer un document en fonction de ce que vous voulez en faire. Vous pouvez choisir le format Open Document si vous voulez que votre fichier soit pérenne ou si vos correspondants utilisent des logiciels capables de le lire. Si en revanche vous connaissez les logiciels de votre correspondant, choisissez un format qu'il sera capable d'utiliser (ou encouragez-le à utiliser la suite libre et gratuite LibreOffice).

16. `http://www.zdnet.fr/actualites/l-etat-francais-a-paye-539-millions-d-euros-a-microsoft-pour-ses-logiciels-en-2011-39790384.htm`

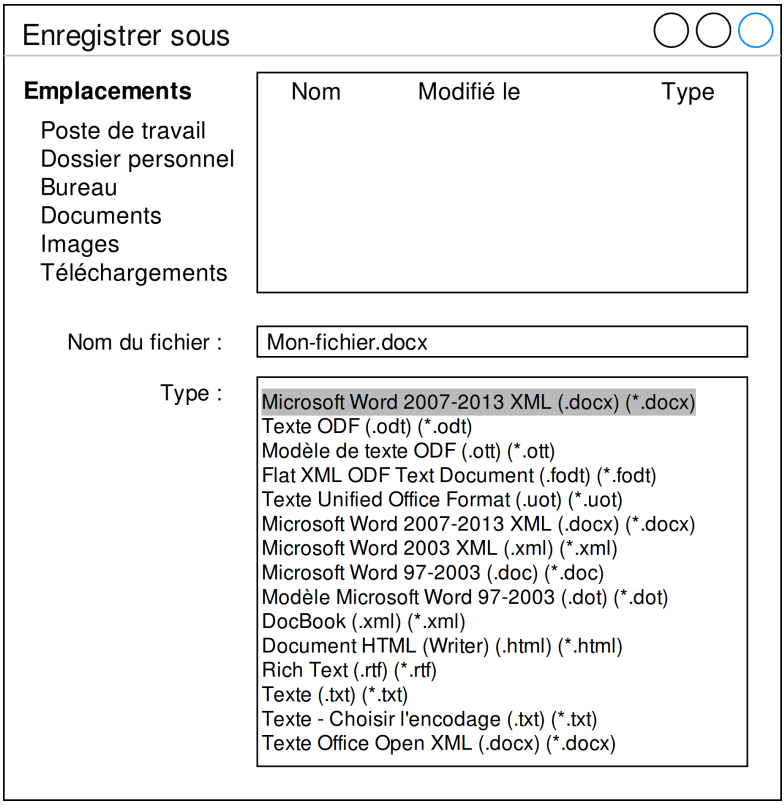


FIGURE 1.4 – Choisir le format de fichier au moment de l'enregistrement

1.6.1.2 Utiliser le format PDF

Un autre moyen d'assurer l'interopérabilité est d'utiliser un format indépendant du logiciel avec lequel vous créez ou lisez un fichier. Il en va ainsi du format PDF, créé par la firme Adobe mais devenu une norme ISO. Tous les lecteurs PDF ne respectent pas cette norme, mais dans le cas de documents « simples », l'envoi au format PDF vous assure une certaine similitude entre ce que vous désirez que votre correspondant puisse voir et ce qu'il verra effectivement. De la même manière, vous pouvez manipuler un fichier PDF sur plusieurs machines et systèmes différents, notamment pour vos diaporamas : avec LibreOffice Impress, vous pouvez sauvegarder votre présentation en PDF et la lire le moment venu avec un lecteur PDF en mode plein écran.

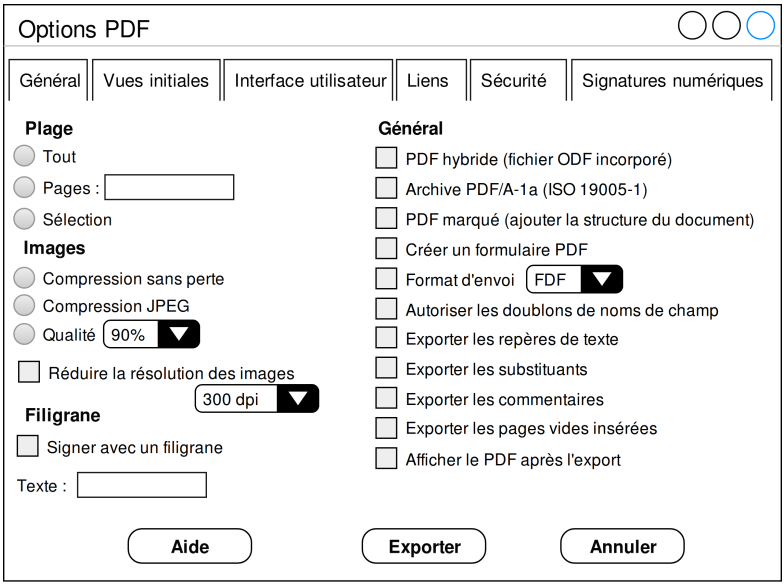


FIGURE 1.5 – Les options PDF pour l'export dans LibreOffice

Avec LibreOffice, l'utilisation du format PDF est intégrée et particulièrement efficace. On peut noter :

— la possibilité de compresser les images, de manière à ce que votre document ne soit pas trop lourd pour un affichage écran (surtout si vous n'avez pas travaillé les images avant de les inclure dans votre document),
— la possibilité d'utiliser la norme ISO,
— la possibilité d'intégrer le document source au format ODF dans le PDF, de manière à pouvoir éditer le document par la suite.

Pour créer un PDF avec LibreOffice, rendez-vous dans le menu `Fichier > Exporter au format PDF`, puis sélectionnez les options désirées avant d'enregistrer.

1.6.1.3 Utiliser du texte

Enfin, un troisième moyen pour assurer la pérennité de vos documents, c'est de les produire dans un format texte et de laisser faire le logiciel pour ce qui concerne la mise en page et la production finale. En effet, de plus en plus de logiciels proposent cette possibilité, en particulier les logiciels de prise de notes ou des éditeurs web comme ceux que vous pouvez rencontrer dans des applications comme le réseau social Diaspora* (dont nous parlons dans le chapitre 4).

Qu'est-ce que cela veut dire ? Vous utilisez l'un des formats les plus basiques qui soient pour écrire votre texte avec un *éditeur de texte*, comme le font les programmeurs. Moyennant l'apprentissage d'un langage très simple comme le Markdown, vous laissez le logiciel interpréter ce langage pour produire un document mis en page. Avantages : vous ne vous occupez plus de la mise en page, vous vous concentrez sur ce que vous écrivez, vous savez que vous pourrez toujours récupérer votre production car elle est au format texte, le format de sortie est généralement interopérable [17].

L'exemple du Markdown est éloquent. C'est une solution de traitement de texte qui nécessite un temps d'apprentissage d'environ 5 minutes. Voici quelques exemples.

17. Sur le même principe, pour des utilisateurs plus avancés, il existe des distributions de LaTeX (voir latex-project.org/ [18]), à la fois langage et système de composition de document très puissant, utilisé notamment pour composer des documents scientifiques des essais…

Pour écrire un paragraphe, vous écrivez « au kilomètre » et vous passez une ligne entre chaque paragraphe en appuyant sur la touche `Entrée` ; pour écrire un mot en italique, vous l'entourez d'une astérisque de chaque côté, pour l'écrire en gras, c'est deux astérisques. Pour créer un lien on utilise des crochets et des parenthèses. Un titre de niveau 1 s'introduit avec un croisillon, un titre de niveau 2 s'introduit avec deux croisillons, un titre de niveau 3 s'introduit avec trois croisillons, etc. Voici un court texte en Markdown :

```
# La fête de Juliette


À l'occasion de la grande soirée donnée en
son honneur au [château de Combrie]
(http://chateaucombrie.com), Juliette remarqua
 la *veste damassée* que portait Nicolas, le
jardinier qui fit tant d'efforts pour paraître
 élégant ce soir-là.

C'est bien lui qui avait successivement ramassé
 et soigné :

* un petit écureuil roux,
* une mésange charbonnière,
* Gaston, le hérisson.
```

Pour écrire en Markdown, le mieux est d'utiliser un logiciel disposant d'un système de coloration syntaxique (vous visualiserez alors mieux les marques de formatage), et éventuellement un panneau latéral permettant de visualiser en direct un aperçu de mise en page. Il existe beaucoup d'éditeurs Markdown. En voici trois assez différents, et libres :

— Ghostwriter [19], un éditeur de texte couplé à un panneau de visualisation directe ; il permet aussi d'exporter aux formats ODT, PDF et HTML,

19. http://wereturtle.github.io/ghostwriter/

— Retext [20], un éditeur similaire à Ghostwriter,
— Stackedit.io [21] : une interface web qui transforme votre navigateur en éditeur Markdown,
— Typora [22] : un éditeur qui intègre le résultat des commandes Markdown à la volée.

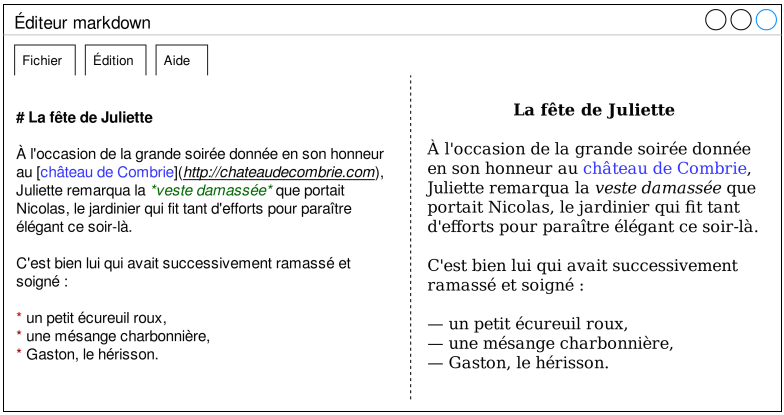


FIGURE 1.6 – Éditeur Markdown et panneau de visualisation de la mise en page en HTML

1.6.2 Manipulation d'images

Les différences de formats de fichier d'image ne sont pas faciles à comprendre. Si vous ne les connaissez pas, il vous sera difficile de les manipuler, ce qui est paradoxal à l'époque où tout le monde peut prendre des photos de grande qualité grâce à toutes sortes d'appareils numériques. Par exemple, si vous destinez une photographie à n'être vue que sur un écran d'ordinateur, il ne vous est pas nécessaire de l'envoyer en haute définition à votre correspondant. Si au contraire vous voulez faire développer une photographie, ou si vous devez imprimer une image sur un poster, il va

20. `https://github.com/retext-project/retext`
21. `https://stackedit.io/`
22. `https://typora.io`

falloir faire attention à sa définition, son contraste, son degré de compression, etc.

Beaucoup de surprises seraient évitées si ces formats de fichiers étaient utilisés à bon escient. Nous procédons à un comparatif dans le tableau 1.2.

Comme on le voit, ces formats de fichiers d'image sont adaptés à différents usages. Là aussi, plusieurs logiciels libres sont à votre disposition :

— GIMP [23] (GNU Image Manipulation Program) : un logiciel d'édition et de retouche d'image. Il permet de manipuler un très grand nombre de formats d'images. Le format de sauvegarde est XCF (afin de sauvegarder un travail en cours), mais il est possible d'exporter dans n'importe quel format. C'est l'outil idéal, par exemple, pour convertir d'un format à l'autre.

— Rawtherapee [24] : il permet de travailler avec des images RAW, c'est à dire directement sorties de votre appareil photo, avec toutes les options pour changer les paramètres.

— Luminance HDR [25] : il permet de traiter des images en vue de pratiquer de l'imagerie à large gamme (*High dynamic range*).

— Inkscape [26] : un logiciel spécialisé dans l'édition de format SVG, idéal pour créer des graphismes adaptés à toutes sortes d'usages : web, impression, iconographie…

Remarque

N'hésitez pas à bien identifier ce dont vous avez besoin. Par exemple, il est possible de traiter des images RAW et même reproduire des effets HDR avec Gimp. Cependant, ce n'est pas son activité de prédilection. De la même manière vous pouvez produire du SVG avec Gimp, mais vous pouvez aussi importer une image dans Inkscape et la vectoriser.

23. https://www.gimp.org/
24. http://rawtherapee.com
25. http://qtpfsgui.sourceforge.net/
26. https://inkscape.org/en/

Nom	Ext.	Définition	Dispo.
Joint Photographic Experts Group	jpg, jpeg, JPG, JPEG	Méthode de compression d'une image fixe (matricielle) et restitution. Plusieurs niveaux de compression disponibles altérant ou non la qualité.	Format ouvert (créé par le groupe du même nom)
Portable Network Graphics	PNG	Spécification (et norme) pour Internet, surtout pour des shémas, graphiques, icônes… Permet aussi l'enregistrement de photographies sans perte de données.	Format ouvert (créé par W3C)
Graphics Interchange Format	GIF	Format sans perte moins puissant que PNG. Destiné au web.	Format ouvert (créé par CompuServe)
Tag(ged) Image File Format	TIFF	Un conteneur d'images (à la manière de ZIP), qui peuvent être de différents formats.	Format ouvert (créé par Adobe)
Désignation Raw (brut, en anglais)	raw	Désigne un type d'images au format « natif » issues des appareils numériques avant leur compression éventuelle en JPG. Permet de travailler directement sur l'image telle quelle, et même reprendre une photo en modifiant les paramètres de prise de vue.	N/A
Scalable Vector Graphics	SVG	Format de *données* pour graphismes vectoriels. Il s'agit de code XML qui *décrit* le graphisme. L'échelle ne change pas la qualité du rendu affiché.	Format ouvert (créé par W3C)

TABLEAU 1.2 – Comparatif de quelques formats d'image

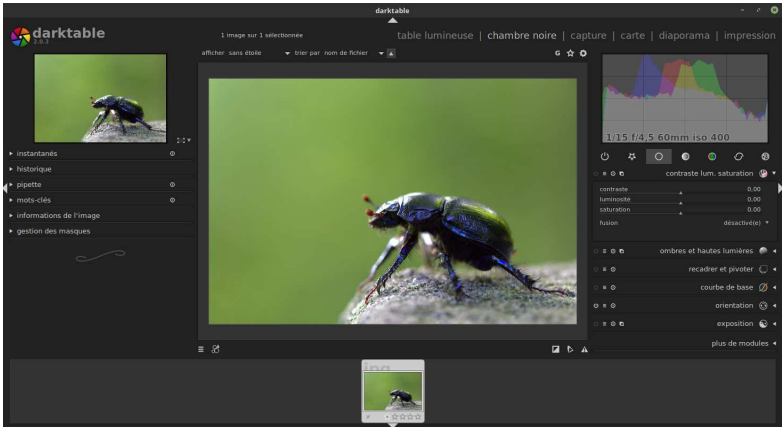


FIGURE 1.7 – Traitement d'image RAW avec Darktable sous GNU/Linux

1.6.3 Audio et vidéo

Tout comme les formats de fichiers d'images, les « formats » audio et vidéo correspondent à des usages différents. Même si cette appellation est générique, vous avez certainement entendu parler de *codecs* à l'occasion d'une lecture d'un fichier audio ou vidéo. Un codec est un dispositif (logiciel) servant à compresser ou décompresser un signal numérique, avec plus ou moins d'efficacité, avec plus ou moins d'options. Par exemple un codec vidéo peut avoir des outils algorithmiques capables de compenser les effets de traînée, ou corriger des mouvements au quart de pixel.

Un logiciel de lecture vidéo ou audio (ou d'image) a besoin des codecs correspondant aux types de fichiers qu'on veut lui faire lire, y compris si les fichiers se trouvent en ligne et accessibles via le navigateur (ce dernier fait appel au programme utile en temps voulu). En l'absence de codecs adéquats, le fichier ne pourra pas être lu.

Certains codecs sont libres, d'autres sont seulement ouverts. Il faut aussi distinguer les codecs qui donnent lieu à des extensions de fichiers (comme `.mpg` ou `.mp3`) et les *conteneurs* qui sont des fichiers (reconnaissables à leurs extensions propres, comme `.avi` ou `.mkv`) mais qui en fait contiennent des fichiers multimédias qui sont

Nom	Nature	Définition	Disponibilité
Xvid	Codec	Norme MPEG (compression)	Libre
DivX	Codec	Norme MPEG (compression)	Ouvert et non-libre
MPEG 1, 2, 4, 7, 21 (Moving Picture Experts Group)	Norme	Normes audio et vidéo concernant le stockage, l'encodage, la diffusion…	Ouvert et non-libre
MP3 (MPEG-1/2 Audio Layer III)	Format	Couche de la norme MPEG-1 pour la compression audio	Ouvert et non-libre
AVI (Audio Video Interleave	Conteneur	Différents codecs peuvent être encapsulés dans un fichier AVI	Ouvert et non-libre
FLAC (Free Lossless Audio Codec)	Codec	Permet la compression audio sans perte.	Libre
Vorbis (extension `.ogg`)	Codecs et formats	Issu de la fondation Xiph.org qui fournit les codecs et formats OGA (audio) et OGV (vidéo).	Libre
MKV (Matroska)	Conteneur	Différents codecs peuvent être encapsulés dans un fichier MKV	Libre

TABLEAU 1.3 – Quelques codecs et conteneurs multimédia

encodés selon des codecs différents. Par exemple, un fichier `.mkv` peut contenir un film dont le son est encodé en OGG et la vidéo en MPEG.

Dans le tableau 1.3 sont présentés quelques codecs et conteneurs.

Évidemment, il n'est pas facile de s'y retrouver… L'essentiel est de retenir qu'un logiciel qui permet de lire des fichiers multimédia doit aussi intégrer les bons codecs. C'est la raison pour laquelle, sur le mode d'emploi de votre chaîne Hi-Fi ou de votre smartphone, vous avez une liste des « formats » que peut lire votre dispositif (le logiciel installé dedans). Dans le cas des smartphones comme dans le cas des ordinateurs, heureusement, on peut choisir ses logiciels.

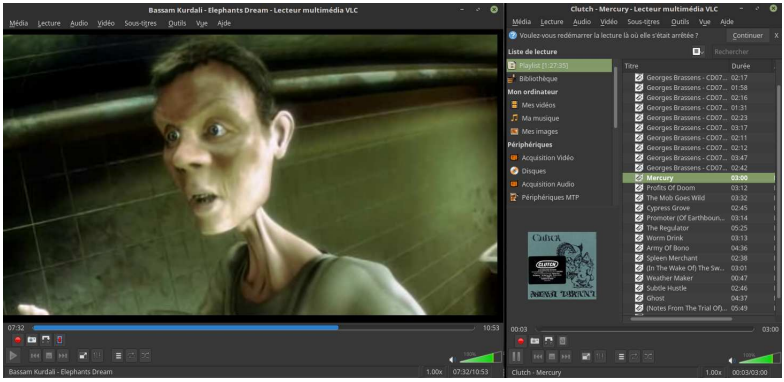


FIGURE 1.8 – Le logiciel VLC

Notez que ce n'est pas parce qu'un logiciel est libre qu'il ne lit que des formats libres. À vous de voir si vous désirez installer des codecs non-libres… tout en utilisant, par exemple, les logiciels libres suivants :

— VLC media player (VLC) [27] : son grand intérêt est qu'il dispose d'emblée d'un très large panel de codecs audio et vidéo, ainsi que sa polyvalence. Son utilisation sur ordinateur, smartphone ou tablette peut aisément remplacer tous les autres logiciels de lecture. Il est de même capable de lire des flux vidéo (comme la télévision en ligne) ou des podcasts, voire devenir un serveur multimédia. Il peut aussi enregistrer… L'installer et l'utiliser par défaut sur votre machine, y compris comme greffon pour votre navigateur Internet, n'est pas un mauvais choix.

— Mplayer [28] ou Smplayer [29] : le second est inspiré du premier. Ils prennent en charge un grand nombre de codecs audio et vidéo, à l'image de VLC.

27. `http://www.videolan.org/vlc/`
28. `http://mplayerhq.hu`
29. `http://smplayer.sourceforge.net/`

— Amarok [30] est un lecteur audio disposant d'une interface facile à prendre en main. Il dispose de greffons très intéressants comme celui qui permet de récupérer sur Wikipédia diverses informations sur l'artiste que l'on écoute.

1.7 Les protocoles sur Internet

Pour terminer ce chapitre sur les logiciels et les formats, il est indispensable de parler des dispositifs techniques sans lesquels la communication informatique ne pourrait pas s'effectuer. Les protocoles dont nous allons parler sont les protocoles réseau, ils sont regroupés sous le nom de suite TCP/IP et ce sont sans doute ceux dont vous entendrez le plus parler si vous cherchez à établir une connexion Internet. Tout comme les formats, il est important de comprendre que ces protocoles de communication sont des standards : déjà présents dès l'origine d'Internet, c'est grâce à eux que le réseau s'est construit.

Bon à savoir

Un protocole de communication est une série d'étapes à suivre pour :

1. établir une connexion avec une autre machine,
2. définir la manière dont les informations seront échangées.

TCP/IP est une suite de protocoles internet qui porte le nom des deux principaux protocoles TCP et IP. Pour normaliser tous ces protocoles, un modèle de connexion entre ordinateurs a été développé par l'ISO sur la base de TCP/IP et nommé le *modèle OSI* (Open Systems Interconnection).

Pour résumer rapidement TCP/IP, on peut dire que cette suite de protocoles est organisée en plusieurs niveaux (couches) qu'on peut représenter sous la forme du tableau suivant :

30. `https://amarok.kde.org/`

	Couche	Exemple	Rôle
5	*Les applications*	HTTP, FTP	Des logiciels permettent d'assurer l'interface homme-machine, comme un navigateur Internet qui envoie et reçoit des requêtes HTTP
4	*Le transports des données*	TCP	Assurer le transport des données (flux). Par exemple : ouverture de la connexion, transfert, fin de la connexion.
3	Le réseau*	IP	La structure du réseau. Pour IP, c'est l'adressage : chaque machine a une seule adresse
2	*Les liaisons*	Ethernet	La méthode de connexion pour transporter les données. Par exemple la commutation de paquets
1	*Couche physique*	ADSL, radio, satellite…	Applications physiques des techniques de communication

TABLEAU 1.4 – Couches de la suite TCP/IP

On peut aussi comprendre cette suite de la manière suivante :

— *l'accès au réseau* (couches 1 et 2),

— *Internet* : une gigantesque ville dont IP (Internet Protocol) permet de gérer les adresses de chaque machine en assurant une fonction de *routage* (on parle alors des *adresses IP* qui identifient les machines sur le réseau),

— *le transport des données* : TCP (Transmission Control Protocol) transporte les données, les découpe en paquets, contrôle leur réception, rend fiable les transferts d'informations,

— *les applications* permettent de traiter les données reçues et initient les envois éventuels.

Ainsi, lorsque vous naviguez sur Internet, toutes ces opérations doivent avoir lieu. Par exemple :

— votre système d'exploitation peut indiquer qu'il existe une connexion active, mais elle peut seulement concerner les premières couches c'est à dire, par exemple, la connexion entre votre machine et la box Internet de votre fournisseur d'accès. Cela ne signifie donc pas pour autant que vous êtes

connecté au réseau Internet (seulement votre « réseau domestique » : vous avez bien une IP du type 192.168.1.XX mais votre box, elle, n'a pas d'IP qui lui permet d'être identifiée et de vous renvoyer des données) ;
— vous pouvez avoir une connexion au réseau Internet mais si la couche applicative fonctionne mal (si votre navigateur est mal configuré) vous ne recevrez rien : pourtant vous êtes bel et bien connecté ;
— d'autres problèmes peuvent survenir dans les couches intermédiaires, par exemple un routeur qui fonctionne mal et renvoie des paquets de manière erratique, etc.

D'autres protocoles de communication existent, nous en verrons davantage dans les chapitres suivants. L'essentiel, ici, est d'avoir une première approche du fonctionnement général d'Internet. C'est sur ce sujet que porte le reste de l'ouvrage. Dans la mesure où les autres couches sont des standards et sont censées assurer les niveaux et qualités de connexion des machines, la couche applicative (les logiciels que vous utilisez) vous concerne en tant qu'individu. C'est essentiellement à travers elle que vous pouvez agir sur le réseau, veiller sur la sécurité de vos données, choisir ce que vous recevez et ce que vous envoyez, prendre garde à ce que devient votre intimité numérique. Vos pratiques sont donc essentielles car elles déterminent votre mode d'existence sur un réseau dont nous venons de voir qu'il n'a rien de virtuel…

1.8 Un système d'exploitation

Pour faire fonctionner les programmes (et les dispositifs matériels) les uns avec les autres, vous avez besoin d'un système d'exploitation (OS pour *Operating System* en anglais) qui regroupe les programmes nécessaires pour accomplir ces tâches. À l'achat de votre ordinateur, vous avez sans doute accepté que soit fourni l'OS. Bien sûr, cette vente liée vous permet d'avoir un ordinateur prêt à l'emploi une fois rentré chez vous. Sachez néanmoins que rien ne

vous oblige à acheter une machine et un système d'exploitation imposé.

Que vous souhaitiez installer Microsoft Windows, Mac OS (pour une mise à jour) ou GNU/Linux, le niveau de complexité est aujourd'hui similaire. On a longtemps accusé GNU/Linux d'être difficile d'accès, mais ces 10 dernières années ont vu fleurir des distributions de GNU/Linux spécialement adaptées au grand public. Dès lors, rien ne s'oppose vraiment à ce que vous choisissiez d'utiliser GNU/Linux, d'autant plus que si vous utilisez déjà des logiciels libres, le changement ne sera pas très difficile.

Qu'est-ce qu'une distribution ?

GNU/Linux a ceci de particulier qu'on en parle en termes de *distributions*. Dans le secteur logiciel, une distribution est un ensemble cohérent de logiciels prêts à installer. Une distribution GNU Linux est la plupart du temps composée des éléments suivants :

- un noyau de système d'exploitation nommé Linux,
- des programmes libres issus du projet GNU,
- des programmes libres différents selon les distributions et qui leur donnent leurs saveurs particulières.

Il existe une multitude de distributions GNU/Linux différentes[31], avec des noms plus ou moins exotiques : Debian (sur laquelle sont basées beaucoup de distributions), Ubuntu, Fedora, Redhat, Suse, Linux Mint, Mageia… Elles ont aussi des bureaux (interfaces) différents, certains rappellant parfois ce que vous connaissez déjà, d'autres qui nécessitent un peu d'apprentissage… tout comme vous avez dû apprendre à vous servir de Windows 98, Windows 2000, Windows 7, Windows 10… Renseignez-vous sur ces distributions avant d'arrêter votre choix ou essayez-en plusieurs.

31. Voir la page Wikipédia « Distribution Linux[32] » qui recense les principales distributions GNU/Linux.

1.9 Je veux essayer GNU/Linux

Dans cette section, nous allons tâcher de décrire rapidement les principales étapes pour installer un système GNU/Linux sur un ordinateur (ici pour la distribution Linux Mint[33]). Si vous ne souhaitez pas le faire, sautez cette section, vous pourrez toujours y revenir.

1.9.1 Vocabulaire

— *image ou fichier iso* : il s'agit d'un fichier archive qui est une copie conforme d'un disque. Le fichier iso se manipule habituellement tel quel. Les distributions GNU/Linux sont presque toujours disponibles en tant que fichier iso. Cela permet de les graver sur un CD-rom ou de créer une clé USB afin d'essayer et d'installer la distribution choisie.

— *Clé USB bootable* : le boot est la procédure d'amorçage d'un ordinateur. Un programme de boot est le programme initial que la machine va exécuter lorsqu'on la démarre. Une clé USB ou un CD-Rom bootable sont généralement des images disque fonctionnant de manière autonome. La machine démarre dessus et on peut ainsi tester le système d'exploitation présent sur le support. C'est encore le meilleur moyen de tester une distribution GNU/Linux (sans toucher au système existant de la machine présent sur son disque dur). D'un point de vue pratique, il est plus rapide de tester et d'installer à partir d'une clé USB car la vitesse de lecture sur ce support est généralement plus rapide que celle d'un lecteur de CD-rom (cela dépend aussi de la quantité de mémoire vive de la machine).

— *Un bureau* : il s'agit d'un agencement de fenêtres et de menus. Les habitués de Windows connaissent différents bureaux, depuis windows 98, en passant par Vista, windows

33. `http://www.linuxmint.com/`

Seven, 8 10, etc. Avec une distribution GNU/Linux, un bureau par défaut est installé mais on peut en changer simplement en installant celui de son choix. Certains bureaux sont graphiquement chargés, d'autres moins, plus ou moins gourmands en ressources, certains sont très ergonomiques, d'autres ressemblent à des terminaux dignes des années 1950, etc.

1.9.2 Objectif

Nous souhaitons installer la distribution Linux Mint sur la machine après l'avoir testée grâce à une clé USB.

Pourquoi Linux Mint ? C'est une question de préférence. Comparer différentes distributions se fait avant tout en fonction des besoins recherchés. Ici nous avons besoin d'une distribution généraliste et polyvalente. Linux Mint propose un bureau nommé Cinnamon, assez simple à appréhender pour commencer, et facilement configurable (il est toutefois possible d'en changer, y compris en prenant une version différente de Linux Mint (bureaux MATE, XFCE…)

1.9.3 Matériel

Nous avons besoin :
— d'une clé USB vierge de 4Go, ce qui suffira amplement,
— d'un ordinateur doté ou non d'un système d'exploitation.

1.9.4 Condition

Si vous possédez Windows il se peut que vous souhaitiez installer GNU/Linux « à côté de Windows ». Nous ne traiterons pas de cette situation dans ce chapitre. Cela dit, pour expliquer rapidement : lors d'une installation normale, si la préexistence de Windows est détectée, le choix vous sera proposé par l'assistant, et le reste de l'installation se fera la plupart du temps de manière très aisée. Cependant, il est conseillé d'avoir une version de Windows la plus propre possible, défragmenter le disque au maximum (voire

ré-installer Windows complètement), avant de procéder à l'installation de GNU/Linux.

Cette cohabitation des deux systèmes sur une même machine se nomme « dual boot ». C'est au démarrage de la machine qu'on devra choisir quel système lancer. Reportez-vous à de nombreux tutoriels sur Internet, afin d'en savoir davantage.

1.9.5 Les étapes

1.9.5.1 Télécharger la distribution

Téléchargez l'image ISO de Linux Mint en 32 ou 64 bits, selon la machine. Si vous ne savez pas si votre processeur est en 32 ou 64 bits, renseignez-vous ou prenez la version 32 bits.

Sur la page de téléchargement[34] des versions de Linux Mint, vous avez le choix entre télécharger des versions 32 ou 64 bits équipées de bureaux différents : Cinnamon, MATE, KDE, Xfce. Cliquez sur votre choix. Une liste de miroirs sera alors proposée, choisissez le miroir le plus proche de chez vous et commencez le téléchargement.

1.9.5.2 Vérifier

Une fois l'iso téléchargée, il faut vérifier l'intégrité de l'image pour ne pas avoir de surprise lors de son utilisation. Cette opération est très rapide, optionnelle, mais d'une prudence élémentaire. Sur la page des miroirs vous avez un lien `Verify your ISO` : il vous mènera vers les sommes de contrôle à vérifier. Il s'agit en gros d'une série de caractères qui attestent l'intégrité de l'image que vous venez de télécharger. Le but du jeu est de tirer la somme de contrôle du fichier ISO désormais présent sur votre machine et la comparer avec celle fournie sur le site (en fichier texte). Pour Linux Mint l'algorithme utilisé est SHA256.

Pour effectuer cette vérification, si vous êtes sous Windows, vous pouvez utiliser :

— Quick Hash GUI[35], un logiciel libre,

34. `http://www.linuxmint.com/download.php`
35. `https://sourceforge.net/projects/quickhash/`

— Hash Express [36], un logiciel non-libre présent dans le Windows Store.

Téléchargez ensuite les sommes de contrôle présentées sur le site Linux Mint, puis effectuez la comparaison (les logiciels de vérification sont très simples d'utilisation).

1.9.5.3 Installer l'image sur une clé USB

Il vous faut un logiciel qui permet d'installer l'ISO sur la clé en la rendant bootable. Vous pouvez utiliser le logiciel Unetbootin [37]. En fait, ce logiciel permet même de télécharger la distribution de son choix, mais au moins vous aurez fait l'effort d'aller sur le site officiel de la distribution…

— choisissez la version de Unetbootin [38] adaptée à votre actuel système d'exploitation et installez le logiciel,
— branchez la clé USB,
— lancez le logiciel Unetbootin,
— sélectionnez l'iso précédemment téléchargée,
— assurez-vous que le bon lecteur usb est sélectionné,
— lancez la procédure.

> **Remarque**
>
> D'autres logiciels pour Windows permettent de créer de telles clés USB. On parle alors de distributions *live* :
>
> — Linux Live USB Creator [a] (LiLi),
> — Multisystem [b],
> — ou vous pouvez acheter directement une clé prête à l'emploi, par exemple sur le site En Vente Libre [c].
>
> *a.* `http://www.linuxliveusb.com/fr/home`
> *b.* `http://liveusb.info/dotclear/index.php?pages/Pr%C3%A9sentation`
> *c.* `https://enventelibre.org/47-cles-usb`

36. `http://www.ecodified.com/ehashfast`
37. `http://unetbootin.sourceforge.net`
38. `http://unetbootin.sourceforge.net`

1.9.5.4 Amorcer

Vous voici avec une clé chargée de potion magique : vous pouvez l'utiliser sans toucher au disque dur de l'ordinateur.

Branchez-la sur le PC sur lequel vous voulez installer GNU/Linux. Assurez-vous que ce PC est bien connecté à Internet (en filaire si possible parce que, même si la puce wifi a de grandes chances d'être correctement détectée lors de l'installation, le wifi est quand même moins rapide). Démarrez le PC.

Et là…

Il y a des chances qu'il démarre sur Windows (s'il en est équipé). Eh oui : chez certains fabricants, il y a une tendance à croire que toute la machine appartient à Windows, donc on ne cherche pas à permettre à l'utilisateur de choisir l'emplacement depuis lequel il veut que la machine démarre.

En fait, au démarrage de la machine, on voit souvent apparaître (rapidement) la possibilité d'appuyer sur une touche (type `F2` ou `F12`, ou `<esc>` / `Échap`, etc.) pour accéder au bios. Parfois même certains fabricants proposent une touche permettant d'accéder directement à un menu de `boot` permettant de choisir le support bootable.

Il faut donc être rapide et presser sur la bonne touche lorsque c'est proposé au démarrage. Si on accède au bios, tout dépend de sa configuration, mais généralement il y a un endroit où l'on peut choisir la séquence d'amorçage. En d'autres termes, il s'agit de dire à la machine : « lorsque tu démarres, tu vas d'abord chercher sur tel support s'il y a un système, et en l'absence de ce dernier, tu cherches sur un autre support ». On peut ainsi agencer (souvent avec les flèches du clavier) la séquence d'ordre de démarrage entre le disque dur, l'USB, le lecteur CD-Rom, etc. Dans notre cas, nous mettrons le disque USB en tête de liste, puis `save and exit`. Pas de panique : à l'avenir, si on a une clé USB branchée lors du démarrage de la machine, dans la mesure où elle ne contient aucun programme d'amorçage, elle sera ignorée. Par contre celle que nous venons de créer avec Unetbootin, elle, contient un programme d'amorçage.

En redémarrant la machine, magie ! c'est le menu de Unetbootin qui apparaît. Il propose alors de tester Linux Mint ou de l'installer, etc.

1.9.5.5 Essayer GNU/Linux

Le mieux est encore de tester. Outre le fait que vous pouvez ainsi essayer la distribution (elle sera alors dans la langue par défaut, c'est à dire souvent en anglais), vous pouvez aussi voir si elle fonctionne bien avec la machine.

Pour l'installation, soit vous la lancez depuis l'interface de Unetbootin, soit (si vous êtes en train de tester) en cliquant sur l'icône d'installation présente sur le bureau.

1.9.5.6 Installation

La première chose qui sera demandée est de sélectionner la langue. Ensuite, il suffit de suivre les fenêtres qui s'afficheront. Tout est fait de manière très intuitive. Attention : lorsque le choix se présentera, n'oubliez pas de retenir attentivement votre login et votre mot de passe, car ils vous serviront pour administrer la machine.

Nous n'irons pas plus loin dans la procédure d'installation. Ici, le cas le plus simple est une machine sur laquelle vous allez *remplacer* votre actuel système d'exploitation par le nouveau. Évidemment, selon votre configuration, des choix plus spécifiques peuvent se présenter :

— si vous avez deux disques durs,
— si vous voulez installer GNU/Linux « à côté » d'un autre système comme Windows,
— si vous voulez partitionner votre disque de manière spécifique…

Dans tous les cas, ne vous lancez pas dans une configuration si vous ne savez pas ce que vous faites. Le mieux est de vous faire aider. Pour cela, vous avez certainement près de chez vous un ou plusieurs Groupes d'Utilisateurs de Linux (GUL). Vous pouvez en trouver la liste sur le site de l'Agenda du Libre [39].

39. `http://www.agendadulibre.org/orgas`

CHAPITRE 2

Le web et les contenus

Naviguer sur la Toile, le web (ou le ouèb), l'Internet — peu importe ici (pour l'instant) la manière dont on appelle ce *Réseau* — n'est pas quelque chose d'intuitif. Il n'est pas évident de comprendre comment sont agencés les contenus et par quels procédés je peux non seulement y accéder, mais aussi pouvoir le faire plusieurs fois, les retrouver au même endroit, ou comprendre pourquoi ils n'y sont plus. En somme, il faut expliquer ce que signifie « naviguer » avec un navigateur, ce logiciel indispensable pour passer de l'affichage d'un contenu web à l'autre. Mais tout cela est soumis à certaines règles, à la fois techniques et juridiques.

2.1 L'URL : savoir où je me trouve sur Internet

L'URL (Uniform Resource Locator — littéralement « localisateur uniforme de ressource ») indique l'adresse d'un contenu sur Internet. Imaginez-la comme une véritable adresse postale dans le grand village d'internet.

Le logiciel qui permet de se rendre à cette adresse est le *navigateur*. Il affiche à l'écran le contenu de la page que vous souhaitez voir, tout comme l'adresse de votre maison permet au facteur de savoir exactement à quelle porte sonner.

Sur la plupart des navigateurs, elle apparaît en haut dans un cadre que vous pouvez éditer, c'est-à-dire que vous pouvez directement taper dans l'espace prévu cette adresse si vous la connaissez. On appelle cet endroit la *barre d'adresse* et elle ne doit pas être confondue avec la barre de recherche d'un moteur de recherche qui apparaît souvent en première page lorsque vous lancez votre navigateur.

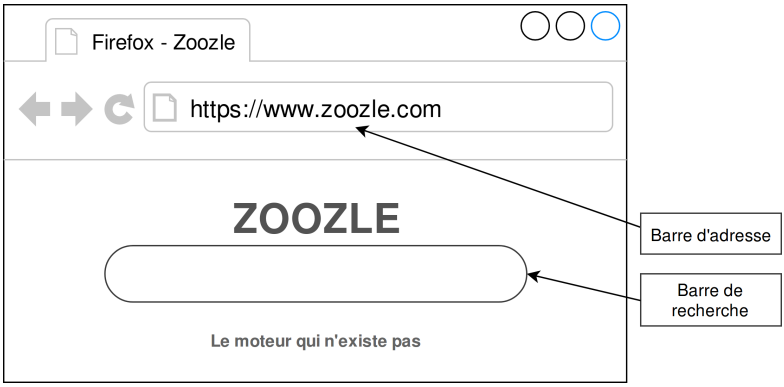


FIGURE 2.1 – Différence entre barre d'adresse et barre de recherche

Pour passer d'un contenu à un autre, d'une page à une autre, on clique sur des *liens*. Un lien est figuré par un texte souligné ou de couleur différente ou encore une image. Dans tous les cas, lorsque le pointeur de la souris est positionné dessus, l'URL de destination s'affiche en bas à gauche du navigateur.

On a tendance à oublier l'affichage de l'URL de destination, car elle se cache souvent derrière le nom littéral des liens des moteurs de recherche et autres sites. Pourtant elle est fondamentale. Lire sa codification n'est pas compliqué et nécessaire pour vérifier la nature de la ressource à laquelle on va accéder en cliquant sur le lien.

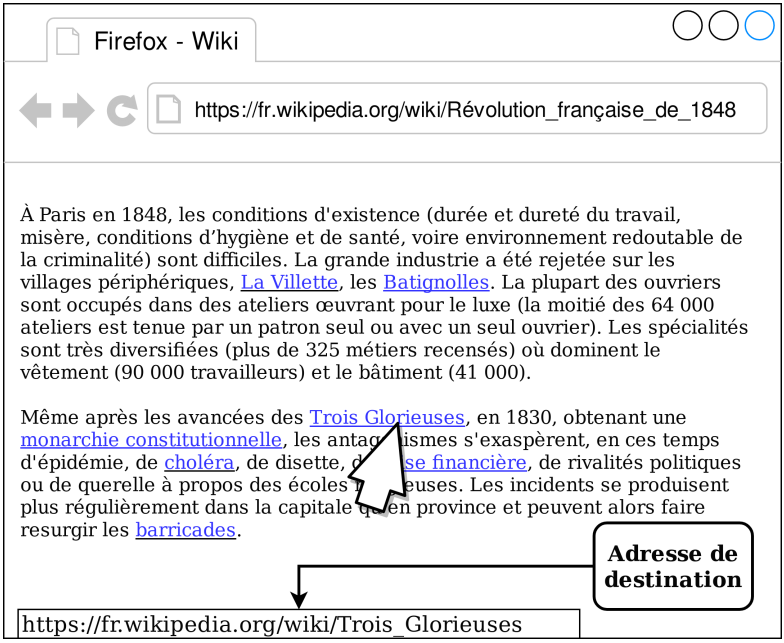


FIGURE 2.2 – URL de destination

2.1.1 Pourquoi les adresses commencent par HTTP ?

HTTP signifie HyperText Transfert Protocol (« protocole de transfert hypertexte »). Comme son nom l'indique, il s'agit d'un protocole technique (des spécifications) qui permet à un programme client (le navigateur, par exemple) et à un serveur (la machine qui héberge le site) de communiquer ensemble. Par ce protocole, lorsque je me rends sur une page de l'encyclopédie Wikipédia, mon navigateur effectue une *requête* auprès du serveur de Wikipédia, il *copie* la page que lui renvoie le serveur (contenus textuels, images, etc.), et il *affiche* la page que je peux lire.

Pour raconter son histoire, le protocole HTTP est la formalisation dans un *standard* du principe de l'hypertexte[1], inventé respectivement en 1945 et 1965 par Vannevar Bush et Ted Nelson. On se trouve là aux origines non pas d'Internet mais du système d'échange d'information en réseau. L'internet que nous connaissons aujourd'hui a du transposer techniquement le concept de l'hypertexte pour l'automatiser à travers le protocole HTTP. Et, bien entendu, il existe plusieurs protocoles d'échange sur Internet. Une variante de HTTP est HTTPS, nous en parlerons plus bas et dans le chapitre 5.

Si on fait le détail, une requête HTTP envoyée par le client consiste à donner au serveur un ensemble d'éléments : la page demandée, les formats d'image acceptés, la langue acceptée, l'identification du navigateur et de sa version, etc. Le serveur, quant à lui (et s'il est bien configuré) renvoie alors des informations qui le concernent, puis ajoute le contenu demandé et si possible de manière à ce que le client puisse le lire correctement en fonction des spécifications qu'il lui a adressé précédemment.

Bref, le serveur vous apporte votre milkshake selon que vous l'avez commandé conformément à la carte des saveurs disponibles et de vos propres goûts. Dans l'illustration 2.3, on voit ce que le navigateur envoie au serveur et ce que ce dernier lui répond avant de donner la page à afficher.

1. `https://fr.wikipedia.org/wiki/Hypertexte`

Ce dialogue est invisible aux yeux de l'utilisateur, mais il donnerait quelque chose comme cela :

Navigateur : — Bonjour, je voudrais recevoir la page Framasoft.org, je suis le navigateur Mozilla Firefox, je tourne sous Linux, je comprends les encodages et les langages que voici.

Serveur : — Enchanté, je peux vous servir. Voici quelques informations sur la manière dont nous préparons votre commande et le fonctionnement de nos cuisines. Ici on fonctionne de manière sécurisée, et d'ailleurs voici un cookie pour accompagner votre commande. Vous trouverez ci-dessous le contenu de la page demandée.

2.1.2 Déchiffrons une URL

Prenons une URL type :
`https://fr.wikipedia.org/wiki/Framasoft`
Que nous apprend cette URL ? Plein de choses...[2]

2.1.2.1 Le plus important : le nom de domaine

`https://fr.` **`wikipedia.org`** `/wiki/Framasoft`

Il s'agit de l'extension (.org, .net, .com, .fr...) précédée d'un identifiant.

L'extension (aussi parfois appelée *domaine de premier niveau*) est l'équivalent du code postal qui localise le quartier où se trouve le site. Le nom de domaine correspond alors à la rue.

Il est bon de savoir que les domaines (et sous-domaines que nous allons aborder ensuite), sont toujours écrits du plus précis au moins précis : ainsi, `fr.wikipedia.org` nous dit que vous visitez le domaine `fr` qui fait partie de `wikipedia`, lui-même étant affilié à l'extension `org`.

2. Merci en particulier à Gee et Pyves pour la contribution à cette section.

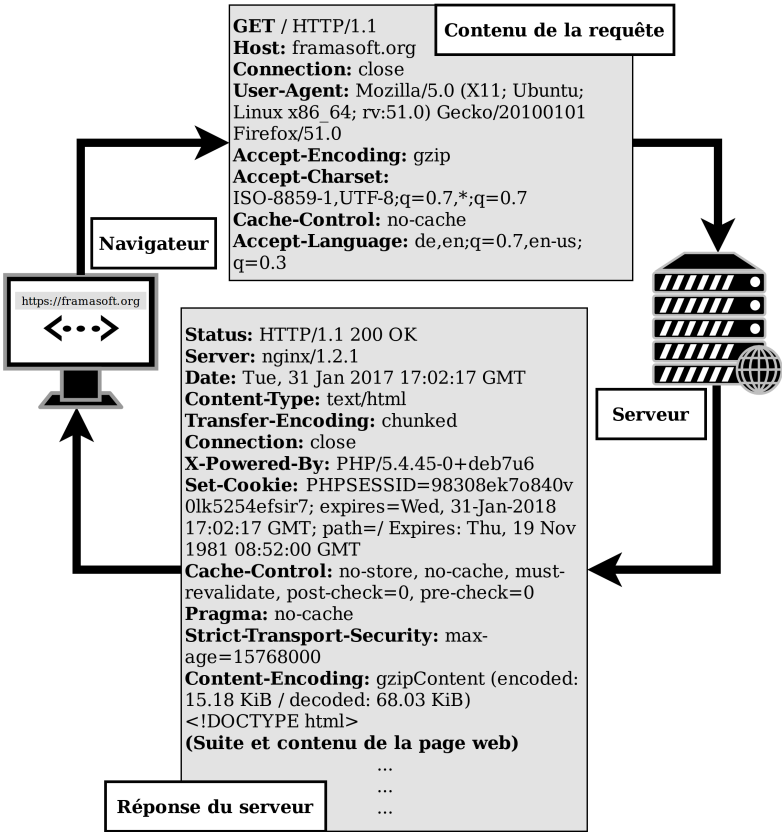


FIGURE 2.3 – Exemple de connexion à la page d'accueil de Framasoft. Requête du navigateur et réponse du serveur

Bon à savoir

Si vous êtes sur une page nommée `wikipedia.bill.com`, vous n'êtes *pas* sur Wikipedia. Vous êtes sur une page appartenant à `bill.com` qui n'a *a priori* rien de commun avec le réseau Wikipedia et qui peut contenir n'importe quoi. Donc *vérifiez toujours que le nom de domaine correspond bien au site que vous souhaitez visiter*.

Les hameçonnages en ligne (*phishing*) fonctionnent souvent de cette manière : vous recevez un courriel avec un intitulé de banque vous demandant d'aller dans votre espace en ligne, avec un lien. Vous cliquez sur le lien et vous arrivez sur un site qui ressemble à s'y méprendre au site de votre banque. Une simple vérification de l'URL permet de déjouer le piège : votre banque devrait avoir un nom de domaine de type `nom-de-la-banque.com`. Si vous voyez quelque chose comme `nom-de-la-banque.quelquechose.com`, abstenez-vous de cliquer !

Les URL peuvent être longues et incompréhensibles. Heureusement, de nombreux navigateurs comme Firefox mettent le nom de domaine en évidence. Ainsi, la lecture est facilitée et vous pouvez en un coup d'œil savoir où vous êtes.

Concernant l'extension (`.org`), elle peut renseigner sur la nature du site. Voici les plus courantes et leurs usages recommandés :

— `.com` : la plus connue, maladroitement considérée comme celle par défaut. Elle signifie pourtant « commercial » et ne devrait être utilisée que par les sites d'entreprises à but lucratif.

— `.org` : utilisée par les organisations non lucratives (associations, sites communautaires, etc.).

— `.net` : sans signification particulière autre que « site web ». Devrait être utilisée par défaut (page perso, etc.).

— `.fr`, `.de`, `.co.uk`, etc. : extensions spécifiques aux pays. Elles sont gérées par les pays directement et dépendent donc de leurs législations (contrairement aux autres qui sont exclusivement américaines).

Notez qu'il ne s'agit que d'usages recommandés. Ainsi, chacun peut acheter un domaine en `.com` même s'il n'est pas une entreprise et n'a pas de but lucratif. L'extension peut donc vous informer, mais elle n'a aucune valeur dans l'absolu. Le site `http://identi.ca/` n'a par exemple aucun rapport avec le Canada (dont le `.ca` est pourtant l'extension) : l'extension a simplement été choisie pour permettre la composition du mot Identica.

2.1.2.2 Le sous-domaine

`https://` **fr.** `wikipedia.org/wiki/Framasoft`

Il s'agit du mot juste avant le nom de domaine.

Si vous savez déjà où vous êtes par le nom de domaine, cette information est moins importante. Néanmoins, elle est aussi une bonne source de renseignements. Ici, vous savez que vous êtes sur la partie francophone de Wikipédia (la partie anglophone serait `en.wikipedia.org`).

Si l'on reprend l'exemple de l'adresse postale : vous avez trouvé la rue *Wikipedia*, le numéro de la maison dans la rue est *fr*.

De nombreux sites permettent une bonne lisibilité grâce à cela. Les services de Google (même si nous ne les recommandons pas) suivent cette logique :

— Google : `https://google.com/`,
— Google Maps : `https://maps.google.com/`,
— Gmail : `https://mail.google.com/`,
— etc.

2.1.2.3 La communication est-elle sécurisée ?

https `://fr.wikipedia.org/wiki/Framasoft`

Le fameux HTTP (cf. ci-dessus) que l'on retrouve en début de chaque adresse désigne les règles utilisées par les ordinateurs pour s'échanger des données sur la toile (pages web, images, vidéos…).

Mais de plus en plus de sites utilisent désormais HTTPS, le S signifiant « sécurisé ». En effet, les pages en HTTPS sont chiffrées avant d'être transmises : votre navigateur et le site se sont mis d'accord sur une manière de chiffrer leurs communications qu'ils sont

seuls à connaître. Une personne qui voudrait espionner la conversation n'y comprendrait rien sans la règle de cryptage.

Grâce à ce sigle, vous pouvez donc savoir très rapidement si les données transitent *en clair* sur le réseau (HTTP) ou non (HTTPS).

Attention : si cela est effectivement un gage de sécurité pour vos communications, cela ne prouve pas pour autant que le site est sûr en tous points. Par exemple, vous ne pouvez pas savoir ce que le site va faire de vos données personnelles : Facebook est accessible en HTTPS mais n'est pas pour autant respectueux de votre vie privée.

Enfin, il pourra vous arriver d'avoir un message d'avertissement lorsque vous vous connectez à une adresse en HTTPS. Nous vous entendons déjà :

> Pourquoi ? si les communications sont sécurisées, n'est-ce pas mieux ?

Oui bien sûr ! Mais HTTPS permet deux choses : tout d'abord de sécuriser ce qui transite dans les tuyaux d'internet, mais aussi garantir que le site que vous visitez est bien authentique. Pour cela, chaque site a enregistré un certificat auprès d'un organisme vérifiant son identité.

Par exemple, lorsque votre navigateur se connecte à Wikipédia en HTTPS, il récupère le certificat du site et demande à l'organisme associé au certificat si celui-ci est authentique. Si ce n'est pas le cas, une page d'avertissement est affichée : les données seront bien chiffrées, mais il est possible que quelqu'un vous fasse croire qu'il est Wikipédia.

Par conséquent, il se peut que vous arriviez sur un site en HTTPS avec un avertissement sur le certificat : si vous n'êtes pas sûr, n'y allez pas !

Nous reprenons ces éléments de sécurité dans le chapitre 5. Reportez-vous y pour plus de détails. En attendant, nous poursuivons notre analyse d'URL.

2.1.2.4 Où suis-je dans le site ?

`fr.wikipedia.org` **/wiki/Framasoft**

Il s'agit du chemin d'accès. Il correspondrait aux indications que vous donneriez au livreur : « Première porte à droite, après l'escalier… ».

Cette dernière information peut également vous servir si le site a une architecture visible. Ici, nous savons que nous parcourons le *wiki* (un gestionnaire de contenus) et que nous sommes sur l'article *Framasoft*.

Cette partie de l'URL est la dernière et n'est pas vraiment normée : certains sites affichent des choses claires comme ici (le nom de l'article est inscrit littéralement dans l'URL), d'autres afficheront des identifiants abscons pour chaque page.

Un petit détail qui peut néanmoins vous sortir de problèmes idiots : si vous avez cliqué sur un lien (dans un forum par exemple) et que la page est inaccessible (erreur 404), vérifiez la fin de l'URL. Il n'est pas rare qu'un lien soit erroné parce qu'il contient un caractère de trop : l'auteur peut avoir malencontreusement inclus la virgule de sa phrase dans l'adresse, provoquant une erreur. Ainsi, si l'adresse finit par `index.html)`, vous pouvez vous attendre à avoir une erreur : retirez simplement la parenthèse à la main et rechargez la page.

2.2 Notions de HTML ou pourquoi le surf n'est pas si simple

Si vous vous souvenez de la question des requêtes HTTP, que nous avons vue ci-dessus, vous n'avez pas oublié que le serveur envoie le résultat de la commande au navigateur de manière à ce que celui-ci puisse l'afficher. Il peut aussi, à défaut, proposer à l'utilisateur un autre programme pour traiter le contenu demandé. Ainsi, par exemple si vous cliquez sur le lien vers un document PDF, c'est le lecteur PDF qui sera sollicité par le navigateur ou bien il vous

sera proposé de télécharger le fichier ou encore de l'ouvrir avec un programme de votre choix.

Pour mieux comprendre comment fonctionnent les pages internet sur lesquelles vous surfez, il faut comprendre comment l'hypertexte est utilisé. Fondamentalement, c'est très simple. L'illustration ci-dessous montre à gauche la rédaction HTML d'une page et à droite le résultat affiché sur un navigateur.

FIGURE 2.4 – Rédaction en HTML

Sans entrer dans le détail, nous allons commenter les différents blocs.

— `<!DOCTYPE html>` : c'est la ligne qui permet de déclarer la grammaire ou la norme du document. Ici nous traitons d'un document rédigé en HTML, mais il y a d'autres possibilités.

— `<html lang="fr">` : nous ouvrons le contenu qui sera encapsulé entre les balises `<html>` et `</html>` tout en indiquant que la langue du document est le français.

— Entre les balises `<head>` et `</head>` nous trouvons, dans l'ordre d'apparition : la déclaration d'encodage (UTF8), le titre de la page, et, entre les balises `<style>` et `</style>`, les styles à appliquer aux différents éléments de mise en page. Par exemple les titres `H1` seront dans la couleur `DeepPink` (rose foncé / magenta). Notons que les styles à appliquer

peuvent être tous regroupés dans un fichier de style à part (il s'agit alors d'un fichier portant l'extension `.css`, pour Cascading Style Sheet).

— Entre les balises `<body>` et `</body>`, nous trouvons le corps du document, c'est-à-dire le contenu informatif qui sera affiché selon les spécifications de mise en page précisées dans les styles.

— `<h1>Chapitre III</h1>` : il s'agit d'un niveau de titre.

— Les balises `<a>` et `</a>` servent à créer des liens. Ici le lien est le mot « terri » et la cible est une page Wikipédia.

— Les balises `<p>`, `</p>` et `<em>`, `</em>` sont relatives à la mise en page et la typographie, elles indiquent respectivement le début et la fin d'un paragraphe, et le début et la fin d'une emphase (italique).

— Enfin, la balise `<img>` sert à traiter des images. Ici nous insérons (avec `src=`) une image en indiquant le nom du fichier.

Bien sûr, cet exemple de page web est simplissime. Mais nous voyons déjà que pour lire une telle page dans votre navigateur, il faut :

— que le navigateur et le serveur soient entrés en communication selon un protocole d'accord qui permet au navigateur de récupérer une page du serveur et l'afficher de manière à ce que vous puissiez la lire ;

— que la page soit correctement écrite en HTML (c'est-à-dire que son créateur n'ai pas fait d'erreur en la composant) ;

— que les fichiers auxquels la page fait appel (ici un fichier image et éventuellement un fichier de styles) soient disponibles.

Dans des cas plus complexes, sur la majorité des sites web que vous fréquentez :

— les pages font souvent appel à des bases de données (ne serait-ce que pour entrer un identifiant et un mot de passe pour accéder à des contenus spécifiques) ;

— des technologies autres que le langage HTML sont souvent sollicitées (Javascript, Ajax, PHP… autant de noms barbares

qui ne font que traiter des contenus et des données échangées).

Pour résumer, surfer sur Internet, c'est faire appel à toutes ces techniques, langages, contenus et données, souvent à vitesse grand V, pour lire, écouter, visualiser des contenus gentiment fournis par les serveurs et *copiés* sur votre machine (dans les dossiers de *cache* de votre navigateur). Si vous avez des difficultés à lire un site web et que vous êtes sûr-e de la bonne configuration de votre machine et de votre connexion, c'est parce que ces éléments ne fonctionnent pas toujours en même temps de la meilleure manière, en particulier si le serveur de la base de données tombe en panne ou se trouve ralenti.

2.3 Je dois accepter des conditions d'utilisation

Les conditions d'utilisation des contenus sur Internet concernent à la fois la manière dont les contenus sont accessibles et les conditions d'usage des services qui distribuent ces contenus. Selon quels critères les contenus web sont-ils compatibles avec les technologies que vous utilisez et pourquoi certains sites et services imposent-ils des conditions d'utilisation ? Certains droits d'usage sont cependant beaucoup plus attentifs aux libertés des utilisateurs.

2.3.1 Accès égalitaire : le rôle du W3C

L'un des facteurs qui a contribué à la fois à la croissance de l'économie d'Internet et à l'extension de ses valeurs sociales de partage, c'est la possibilité d'utiliser des protocoles ouverts pour pouvoir communiquer sur le réseau. Sans l'ouverture de ces protocoles, les navigateurs ne pourraient pas tous communiquer de la même manière avec les serveurs, nous ne pourrions pas envoyer de courriels entre abonnés de différents services, il y aurait même peut-être plusieurs réseaux Internet différents sans correspondance entre eux…

Pourtant, utiliser de manière égalitaire des spécifications techniques n'est pas suffisant. Il faut encore que les éditeurs de contenus puissent présenter ceux-ci de façon cohérente, de manière à ce qu'un article mis en ligne en France, soit lisible de la même manière partout dans le monde quelle que soit l'origine de la connexion ou le navigateur employé.

C'est à cela que s'emploie le World Wide Web Consortium [3] (W3C) depuis 1994. Le W3C est un organisme à but non lucratif, possédant des antennes un peu partout dans le monde. Il s'emploie à émettre des recommandations visant à garantir la compatibilité des technologies web, comme le HTML que nous venons de voir dans la section précédente. Il peut s'agir de langages web, de format d'images, de méthodes d'exploitation de bases de données, d'accessibilité, etc. Notez qu'il ne s'agit pas de certification, comme le ferait une instance de normalisation. Le W3C émet des recommandations suivant une méthodologie précise et exigeante : si les éditeurs, fabricants ou développeurs choisissent de ne pas respecter ces recommandations, c'est alors à eux de s'en expliquer, avec tous les risques de rejet que cela comporte.

En la matière, le monde des développeurs web se souvient des frasques de Microsoft Internet Explorer 6, qui avait beaucoup de mal à assurer une compatibilité acceptable avec les contenus. Les développeurs ont même dû créer des solutions complexes de paramétrage pour ne pas pénaliser les utilisateurs d'IE6 qui, autrement, auraient eu de grandes difficultés pour accéder aux contenus.

Aujourd'hui, la mention « ce site est optimisé pour la version Y du navigateur X » a pratiquement disparu, justement grâce aux travaux du W3C. Dès lors, si vous avez des difficultés avec un navigateur récent et dont vous avez assuré la mise à jour, il y a fort à parier que les problèmes d'affichage proviennent des développeurs et non de votre fait.

Néanmoins, des technologies sont souvent utilisées bien qu'elles ne fassent pas partie des recommandations du W3C. C'est le cas de Adobe Flash [4], un logiciel tout droit issu des années 1990,

3. https://www.w3.org/
4. https://fr.wikipedia.org/wiki/Adobe_Flash

qui permet de créer et afficher des applications fonctionnant sur le navigateur disposant d'une extension Flash. Certains sites proposent ainsi des animations, souvent lourdes à charger et dont la fiabilité en termes de sécurité peut laisser à désirer. Il s'agit par exemple de petits jeux en Flash, ou encore d'une animation sur la page d'accueil d'un site (souvent bien inutile). Certains grands éditeurs comme Apple, Google et Microsoft prennent de plus en plus leurs distances vis-à-vis de cette technologie, qui est désormais supplantée par le HTML5 (c'est-à-dire la nouvelle version de HTML qui intègre déjà des couches permettant de développer des applications et afficher, par exemple, des contenus multimédia cohérents et répondant aux spécifications du W3C).

2.3.2 Gérer ses plugins pour choisir ses contenus

Heureusement, les navigateurs disposent de moyens pour décider si l'on veut ou non utiliser de telles technologies. La plupart du temps, les commandes sont directement accessibles dans la fenêtre dès lors que la navigateur fait appel à une extension pour afficher des contenus. Dans le cas de Flash, il faut une extension Flash-Player que l'on peut activer ou désactiver au besoin.

Dans l'illustration suivante, on apprend que les plugins (extensions) en cours d'utilisation sont symbolisés par un petit bloc de Lego dans la barre d'adresse. On peut alors désactiver l'extension si elle est active ou choisir de l'activer si elle ne l'est pas par défaut.

De manière générale, un bon navigateur est un navigateur qui vous permet de choisir les contenus, en particulier lorsque certains vous sont imposés et ne sont pas forcément pertinents pour votre navigation. De bons outils pour cela se nomment *plugins* ou *extensions* ou encore *modules complémentaires* et vous permettent d'étendre les fonctionnalités de votre navigateur.

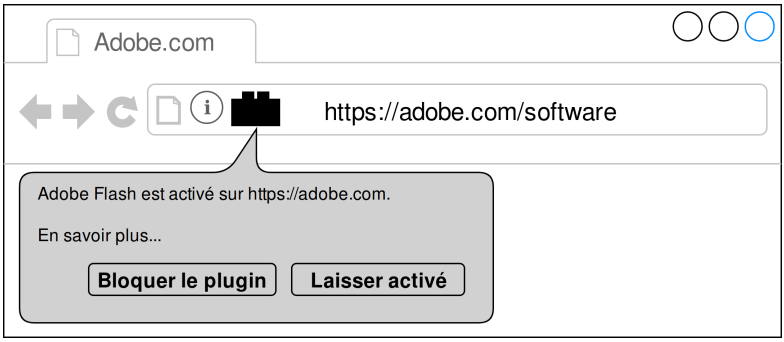


FIGURE 2.5 – Activer ou désactiver le plugin Flash

La fondation Mozilla propose ainsi pour Firefox une pléthore de modules développés par la communauté, et que l'on peut installer facilement [5]. Dans le chapitre 5, par exemple, le module Privacy Badger [6] vous est présenté pour éviter le traçage des sites web et protéger votre confidentialité.

Voici quelques exemples de modules sympathiques :

— pour éviter les publicités intempestives, vous pouvez installer uBlock Origin [7] ;

— pour corriger ce que vous écrivez dans le navigateur (par exemple lorsque vous écrivez un courriel depuis un *webmail*), vous pouvez utiliser Grammalecte [8] ;

— vous pouvez aussi utiliser un service en ligne et établir un pont avec le contenu apparaissant dans le navigateur ; c'est l'exemple de Framabag [9], un service basé sur Wallabag [10] et qui vous permet de stocker en ligne des pages web (comme un article) puis de les consulter plus tard à tête reposée, sur votre mobile, par exemple.

5. https://support.mozilla.org/fr/kb/desactiver-supprimer-modules
6. https://addons.mozilla.org/fr/firefox/addon/privacy-badger17/
7. https://addons.mozilla.org/fr/firefox/addon/ublock-origin/
8. https://addons.mozilla.org/fr/firefox/addon/grammalecte-fr/
9. https://framabag.org/
10. https://wallabag.org/fr

Pour installer un module pour Firefox [11], il suffit de vous rendre sur le site-dépôt des modules [12], choisir un module et cliquer sur « Ajouter à Firefox ». Un script (petit programme) permettra alors à Firefox de télécharger et installer le module.

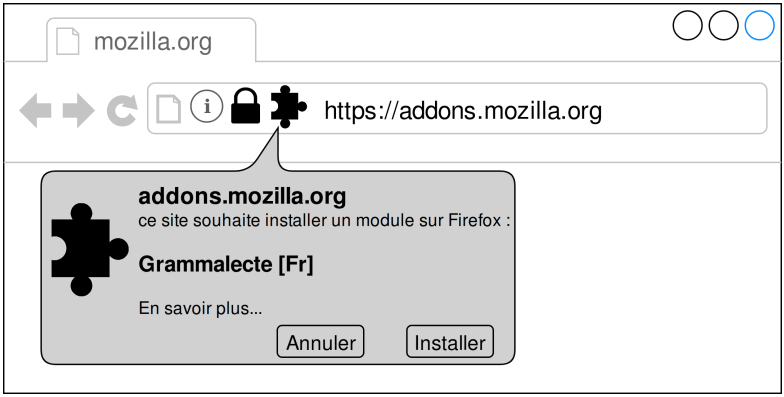


FIGURE 2.6 – Choisir et installer un module

Un autre moyen consiste à se rendre dans le gestionnaire de modules de Firefox et choisir dans le « catalogue ». Pour gérer les modules, les activer, les désactiver, les supprimer, allez dans le gestionnaire de modules puis dans « Extensions ».

FIGURE 2.7 – Gérer les modules

En somme, vous avez compris que les bons usages des technologies web et des navigateurs sont ceux qui vous laissent la liberté

11. https://addons.mozilla.org/fr/firefox/
12. https://addons.mozilla.org/fr/firefox/

de lire des contenus comme vous le voulez. L'ajout de contenus non pertinents, comme des publicités intrusives, peut gâcher votre lecture et vous amène à équiper votre navigateur avec des modules adaptés. Cependant, certains modules, parce que leur fonctionnement implique un traitement des informations, peuvent dégrader la rapidité de votre navigateur. D'autres modules sont en revanche très utiles, permettent davantage de confort et sont même parfois addictifs.

2.3.3 Les Conditions Générales d'Utilisation (CGU)

Les CGU se trouvent généralement par un lien en bas de page du site que vous consultez ou du service que vous utilisez. Pourquoi existe-t-il des CGU ?

Il s'agit d'abord d'un *contrat* entre l'éditeur et l'utilisateur qui vise à mettre au clair les conditions dans lesquelles l'éditeur met un contenu ou un service à disposition et celles dans lesquelles un utilisateur est en mesure d'en user. Les CGU déterminent alors les *responsabilités* de l'un et de l'autre et peuvent aussi mentionner des sanctions éventuelles.

Par exemple, un forum peut rappeler dans ses CGU que les propos racistes et injurieux sont punis par la loi, il peut stipuler que l'éditeur ne saurait être tenu responsable des propos écrits par les membres mais que ces derniers peuvent se trouver bannis du forum au cas où ils écriraient de tels propos.

Le fait d'utiliser un site ou un service équivaut à accepter les CGU, mais bien peu d'internautes prennent le temps ne serait-ce que survoler ces textes.

Prenons l'exemple des CGU de Google. On ne peut pas reprocher à cette firme d'être opaque sur ses CGU puisqu'elle les rappelle régulièrement via un message d'alerte lorsque vous effectuez une recherche sur son site le plus utilisé, son moteur de recherche. Dans les CGU de Google [13], on trouve [14] :

13. `http://www.google.com/intl/fr/policies/terms/`
14. CGU consultées le 01/02/2017.

> Certains de nos Services vous permettent d'importer, de soumettre, de stocker, d'envoyer ou de recevoir des contenus. Vous conservez tous vos droits de propriété intellectuelle sur ces contenus. En somme, ce qui est à vous reste à vous.
>
> Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus. Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services [...].

Il est vrai que la tournure est parfois alambiquée. Ici, on peut imaginer une certaine contradiction entre les deux paragraphes, l'un stipulant que nous conservons tous nos droits sur nos données, et l'autre impliquant que Google peut en faire à peu près ce qu'il veut. En réalité, vous conservez effectivement tous vos droits sur les données, mais le fait d'utiliser les services de Google implique que vous donnez une licence d'usage à Google et que cette licence n'est pas censée prendre fin, même si vous n'utilisez plus les services en question.

Notez aussi que, selon le pays du site ou du service que vous utilisez, les CGU peuvent non seulement être rédigées dans une langue que vous ne comprenez pas, mais aussi emporter des conditions parfaitement légales dans le pays en question et non dans le

vôtre. Dans ce cas, tout contentieux risque d'être bien difficile à résoudre (ceci sans compter le lieu où vos données sont stockées, en particulier si les serveurs ne sont pas sur le sol français).

Les clauses des CGU de Google constituent un cas d'école. Heureusement, tous les sites et services sur Internet n'usent pas de telles libertés qui, si elles sont relativement légales, impliquent cependant des pratiques qui ne sont pas vraiment loyales. En contraste, une association comme Framasoft, qui propose elle aussi des services en ligne et des contenus, affiche des CGU claires et pédagogiques [15] qui stipulent notamment qu'aucune exploitation ne sera faite des données. Les CGU de Framasoft visent essentiellement à rassurer les utilisateurs, agir en transparence et prévenir des risques d'abus.

2.3.4 Cadre légal

Sur Internet, les cas d'abus ne manquent pas. Lors de l'ouverture du service Framasphère [16], un nœud du réseau social Diaspora* [17], l'association Framasoft a du faire face à plusieurs cas de manquement au règlement et à la loi, comme par exemple l'usage non autorisé de photographie d'un tiers, des usurpations d'identité, etc. Heureusement, les coordonnées des responsables du site et leur réactivité ont permis à chaque fois une résolution adéquate des situations. Ce n'est malheureusement pas le cas partout, en particulier s'il s'agit de services aux conditions d'utilisation douteuses.

Tous les sites et services qui enregistrent des données personnelles, ne serait-ce que vos noms et prénoms, doivent faire l'objet d'une déclaration à une autorité qui va étudier à la fois ce que les services font avec ces données, comment ils le font, s'ils les transfèrent ou non dans un autre pays, et les informations qu'ils en infèrent. Pour la France, c'est la CNIL (Commission nationale de l'informatique et des libertés) qui est en charge de traiter et surveiller les déclarations de ce type. Pour les autres pays, vous pouvez vous

15. http://www.google.com/intl/fr/policies/terms/
16. https://framasphere.org/
17. https://fr.wikipedia.org/wiki/Diaspora

reporter à la carte [18] éditée par la CNIL sur son site : en cliquant sur un pays vous pourrez savoir s'il existe une autorité équivalente, quelles sont les dispositions législatives concernées, et les coordonnées des points de contacts officiels.

Pour la CNIL, ce qu'on appelle « données personnelles » est défini relativement à l'article 2 de la Loi Informatique et Libertés [19] :

> Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement.

L'éditeur d'un site ou d'un service, dans la mesure où il utilise des données personnelles de ses utilisateurs, en constitue donc un fichier destiné à être exploité. C'est ce fichier et ses spécifications qui doivent être déclarés. En France, les manquements en termes de conformité CNIL de ces fichiers est punissable de 300 000 euros et de 5 ans d'emprisonnement.

Vous aurez compris qu'avant d'entrer vos données d'identité, votre adresse ou tout autre information personnelle sur un site ou un service, il est de votre intérêt de vérifier auparavant quelques éléments :

— si l'éditeur a enregistré son site ou son service auprès de la CNIL ou un équivalent dans le pays concerné. Généralement, la mention de l'enregistrement et même le numéro sont accessibles dans la partie « À propos » ou « Mentions légales », souvent un lien en pied de page ;

— en cas de doute, vérifiez auprès d'un annuaire pour retrouver l'identité de l'éditeur : une recherche WHOIS [20] (qui est… ?) auprès de l'AFNIC [21], par exemple, vous permet, à partir d'un nom de domaine, de trouver l'identité de celui

18. `https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde`

19. `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460`

20. `http://www.afnic.fr/fr/produits-et-services/services/whois/`

21. L'AFNIC est l'Association Française pour le Nommage Internet en Coopération. Elle se définit ainsi sur son site afnic.fr : « L'Afnic est le centre de gestion (registre) et de ressources des noms de domaine Internet géographiques pour la France

qui a déclaré ce domaine. Cela ne signifie pas pour autant que c'est cette personne qui édite effectivement le site, mais c'est une indication pertinente ;

— renseignez-vous sur les moyens à votre disposition pour effectuer des démarches afin de récupérer vos droits (droit à l'image, droit d'auteur, autres informations personnelles, etc.) : le site de l'éditeur doit mentionner une adresse à laquelle vous pouvez écrire (en conservant une copie de votre message) et sur son site, la CNIL vous donne quelques astuces pour mener à bien ce type de démarche.

2.4 Les droits d'usage

Toute l'histoire d'Internet repose sur les notions de partage : partage du code, partage des connaissances, partage des techniques, et toutes ces conditions qui firent qu'Internet a été construit comme un réseau libre et ouvert. Dès lors, que pouvez-vous faire avec les contenus que vous lisez, copiez ou téléchargez sur Internet ? Cette question est vaste et appellerait un développement bien trop long pour cet ouvrage, surtout parce qu'elle traite du droit d'auteur. Nous allons donc devoir prendre quelques raccourcis : reportez-vous aux références citées si vous désirez en savoir davantage.

2.4.1 Partager ?

Lorsque nous disons qu'Internet a été construit sur des valeurs de partage, que voulons-nous dire exactement ? Non pas que la structure technologique des premiers ordinateurs en réseau ait été développée de manière anarchique, d'autant plus que les premiers projets de développement aux États-Unis ont été en partie portés

(le `.fr`), l'Ile de la Réunion (le `.re`), Saint-Pierre et Miquelon (le `.pm`), Mayotte (le `.yt`), Wallis et Futuna (le `.wf`) et les Terres australes et antarctiques Françaises (le `.tf`). »

par des fonds militaires à la fin des années 1960. Ce que cela signifie, c'est que la communauté des développeurs des protocoles et des programmes qui ont permis de faire fonctionner un réseau et des serveurs, l'a fait dans un esprit d'ouverture.

L'exemple typique est les RFC (Requests For Comments), littéralement, les « demandes de commentaires ». Elles concernent différents aspects techniques d'Internet ou matériels. Ces RFC sont regroupées en une série qui démarre en 1969. Le principe : à l'initiative d'un volontaire (tout le monde peut proposer une RFC), un brouillon est proposé à toute la communauté puis, si ce brouillon retient l'attention et après discussion générale et publique, une rédaction finale est tenue à disposition de tous. Les RFC sont toutes rédigées de la même manière et expriment des exigences (obligations, restrictions, recommandations…). C'est notamment grâce à ce partage des connaissances et des techniques qu'Internet a modélisé tous les outils qui permirent aux utilisateurs de collaborer et construire une communauté mondiale, avec une économie, des entreprises, etc.

Pourtant, dans ce monde de partage, comment comprendre cet apparent paradoxe que tous les partages ne sont pas permis et même sanctionnés par différentes lois ? Plus troublant encore, si l'on considère ce vaste projet de partage qu'est Wikipédia, on apprend assez vite que l'utilisation des contenus de Wikipédia est soumise à certaines contraintes.

2.4.2 Droit d'auteur

Le droit d'auteur[22] est un droit qui s'applique aussi bien sur Internet qu'ailleurs. Simplement, le développement d'Internet a quelque peu bousculé les pratiques.

Le droit d'auteur est acquis de manière automatique dès lors que vous créez une œuvre. Il y a deux acceptions à ce droit d'auteur :

— un droit moral, qui permet d'attribuer à l'auteur la paternité de son œuvre et protège l'intégrité de cette œuvre,

22. https://fr.wikipedia.org/wiki/Droit_d%27auteur

— un droit patrimonial, par lequel un auteur peut diffuser son œuvre ou céder l'exclusivité de la production et de la distribution à un tiers (un éditeur, par exemple).

La diffusion et la multiplication des contenus sur Internet rend plutôt difficile la régulation du droit d'auteur. Si vous vous souvenez des CGU de Google dont nous avons parlé ci-dessus, la jurisprudence peut prêter à sourire si elle ne reflétait de graves difficultés à faire respecter le droit d'auteur sur Internet. Ainsi, le Tribunal de Grande Instance de Paris a jugé une affaire le 9 octobre 2009 [23]. Cette affaire opposait un photographe, une société éditrice de photographie, un site Internet et la société Google Image. Pour résumer : une photographie disponible sur le site a été reprise par Google Image mais le nom de l'auteur n'ayant pas été mentionné, le TGI, sur demande du photographe à déréférencer son œuvre, a condamné Google Image. À travers cette affaire, on voit clairement les difficultés que les auteurs peuvent avoir pour protéger leur droit moral à la paternité (la photographie ayant été retouchée sans mentionner le nom de l'auteur), et même le droit patrimonial (la société éditrice en charge de la distribution de l'œuvre doit elle aussi être de la partie plaignante).

Évidemment on comprend aussi que, étant donné la mondialisation du réseau, les acceptions du droit d'auteur ne sont pas les mêmes dans tous les pays, exception faite des pays signataires de la Convention de Berne [24] qui s'accordent sur une majorité de principes. C'est pourquoi des déséquilibres et des tensions ont cours sur Internet à propos du respect des droits d'auteur, et ne sont pas forcément le fait des piratages et autres pratiques, condamnables, mais dont le caractère illicite est néanmoins très clair… Jusqu'à ce que vous compreniez que dans la mesure où toute consultation de contenu sur Internet est une copie, ce n'est plus seulement l'appropriation illicite d'une œuvre qui est en jeu mais la méthode de sa

23. https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-3eme-chambre-2eme-section-jugement-du-09-octobre-2009/

24. http://www.wipo.int/treaties/fr/ip/berne/

distribution et les droits de diffusion et reproduction (c'est pourquoi les sites pirates sont généralement condamnés pour contrefaçon et non pour distribution illégale de copies).

Concrètement, face à cette complexité, l'utilisateur doit respecter certains principes relativement simples. En voici quelques-uns que vous avez tout intérêt à retenir :

— vous pouvez utiliser une œuvre (un contenu créé par quelqu'un d'autre que vous, qu'il s'agisse de programme, image, texte, etc.), pour la diffuser d'une manière ou d'une autre, uniquement à partir du moment où vous êtes en mesure de savoir que vous avez effectivement le droit d'en disposer, dans quelles conditions et si et seulement si vous en attribuez la paternité à l'auteur (vous citez l'auteur) ;
— vous pouvez citer une partie courte d'un texte (le droit de citation [25] est une exception au droit d'auteur) à la condition d'en attribuer la paternité et d'indiquer la source de l'œuvre,
— vous pouvez indiquer la provenance d'une œuvre sur Internet ou faire un lien vers cette œuvre mais vous n'avez pas la possibilité de vous en autoriser vous-même le droit de diffusion.

Si le respect du droit d'auteur doit s'appliquer sur Internet comme ailleurs, il reste que la concentration des contenus sur Internet par de grands monopoles ont réussi en peu d'années à créer des inégalités et des injustices. On peut se reporter à l'ouvrage de Joost Smiers et Marieke van Schijndel, *Un monde sans copyright et sans monopole* [26], qui, après un état des lieux des distorsions du droit d'auteur par les monopoles économiques (pays ou grandes firmes) propose de se passer complètement du copyright (et donc du droit d'auteur) pour créer un nouveau modèle économique. Pour illustrer cela, on peut citer la concentration des publications scientifiques par de grands éditeurs comme Elsevier, des éditeurs « papier » au départ et qui, après avoir racheté de multiples autres éditeurs, ont créé des monopoles sur l'édition et la distribution (numérique et papier) des publications scientifiques. Aujourd'hui

25. https://fr.wikipedia.org/wiki/Droit_de_courte_citation
26. https://framabook.org/un-monde-sans-copyright-et-sans-monopole-2/

des millions d'euros de fonds publics partent entre leurs mains, ce qui crée une grande inégalité à l'échelle mondiale sur l'accès aux connaissances scientifiques [27].

De nouveaux équilibres du droit d'auteur

Pour favoriser de nouveaux équilibres dans la société numérique, plus pertinents et non moins contraignants, les licences libres (ou ouvertes) permettent d'octroyer *a priori* certains droits aux utilisateurs au lieu de restreindre les usages par défaut. Ainsi, de plus en plus de contenus disponibles sur Internet sont diffusés sous ces licences. Il est important d'en comprendre le sens et les possibilités qui sont ouvertes.

2.4.3 Licences libres

Les licences libres ne concernent pas seulement les logiciels (voir le chapitre 1, où nous définissons une licence libre). Elles dépassent largement le cadre de l'usage des programmes car leur objectif n'est pas seulement de partager un bien mais aussi de partager ce qu'on peut faire de ce bien. Ainsi un morceau musical sous licence libre peut être remixé et re-partagé, un texte peut être traduit (c'est-à-dire modifié) et cette traduction peut être diffusée, etc.

En fait, les licences libres ne s'opposent pas au droit d'auteur — elles tendraient même à le renforcer — mais s'opposent à la notion d'exclusivité et de concentration des droits, pour donner à l'auteur la possibilité de déterminer *a priori* les conditions d'usage de son œuvre. Ainsi, il est non seulement possible de placer une œuvre non-logicielle sous licence libre, mais cela équivaut à une démarche spécifique de l'auteur qui souhaite verser sa production dans les biens communs. Ce faisant, il ne renie pas le droit moral d'auteur car ce dernier est inaliénable : quoi qu'il arrive, l'auteur est toujours reconnu comme auteur, même lui ne peut pas dénier cette qualité (dans l'état actuel du droit).

27. C'est ce qui a poussé des étudiants et des chercheurs à créer Sci-Hub, un portail qui permet d'accéder aux articles scientifiques gratuitement à la manière des sites de piratage de films.

L'encyclopédie Wikipédia est une illustration convaincante de ce que les licences libres permettent non seulement de partager des contenus mais aussi de participer à leur création, qu'il s'agisse de connaissances, d'illustrations, de photographies ou de vidéos. Les contenus de Wikipédia sont placés sous licence *Creative Commons attribution, partage dans les mêmes conditions* : cela signifie que vous pouvez utiliser et partager ces contenus dans la mesure où vous en citez la source et que la licence de ce que vous partagez en provenance de Wikipédia soit cette même licence. En d'autres termes, conformément au droit d'auteur, vous ne pouvez pas vous attribuer la paternité de ce contenu, vous devez citer Wikipédia au titre de cette paternité. Par contre, en plus, vous pouvez modifier ce contenu à condition de renseigner ce que vous avez modifié, et vous pouvez diffuser comme vous l'entendez à condition d'utiliser la même licence.

Désormais, vous savez quoi répondre à votre enfant qui prétend qu'il peut utiliser des contenus Wikipédia pour son devoir d'Histoire : il peut citer, mentionner la source, mais en aucun cas prétendre en être l'auteur. Quant au professeur qui ne supporte pas Wikipédia, vous lui pouvez rappeler que le problème n'est pas dans le fait d'utiliser ou non des contenus de Wikipédia, mais dans le fait de s'attribuer ces contenus sans en citer la source. Vous pouvez aussi ajouter que si les contenus de Wikipédia ne le satisfont pas, il peut lui aussi y contribuer en corrigeant ou créant des notices…

Pour utiliser des contenus sous licence libre, vous devez distinguer les licences entre elles. Pour débuter, il est inutile d'entrer dans le détail, mais sachez simplement que toutes les licences libres imposent des conditions qui ne sont pas tout à fait les mêmes. En général on distingue :

— les licences libres : vous pouvez utiliser, partager, modifier et diffuser la modification, exactement comme s'il s'agissait d'un logiciel libre (cf. les 4 libertés dans le chapitre 1) ;

— les licences libres *copyleft* : *copyleft* est un jeu de mot signifiant *gauche d'auteur* par opposition au *copyright* ; cela signifie que l'œuvre, modifiée ou non, doit être redistribuée exclusivement sous la même licence que celle de départ ;
— les licences de libre diffusion : certaines clauses ne sont pas compatibles avec les 4 libertés, mais l'usage de l'œuvre est tout de même facilité.

Voici quelques exemples de licences pouvant s'appliquer à des contenus culturels, scientifiques ou artistiques :

Nom de la licence	Abréviation	Caractéristique
Licence Art Libre	LAL	Licence libre copyleft
Licence de documentation libre	GNU FDL	Licence libre copyleft
Creative Commons - Attribution	CC-BY	Licence libre non copyleft
Creative Commons - Attribution - Partage des conditions initiales à l'identique	CC-BY-SA	Licence libre copyleft
Creative Commons - Attribution - Pas de modification	CC-BY-ND	Licence de libre diffusion
Creative Commons - Attribution - Pas d'utilisation commerciale	CC-BY-NC	Licence de libre diffusion
Creative Commons - Attribution - Pas d'utilisation commerciale - Partage des conditions initiales à l'identique	CC-BY-NC-SA	Licence de libre diffusion
Creative Commons - Attribution - Pas d'utilisation commerciale - Pas de modification	CC-BY-NC-ND	Licence de libre diffusion

TABLEAU 2.1 – Exemples de licences libres

En guise d'application, voici une bande dessinée sous licence libre CC-By-SA, que nous avons modifié (nous avons traduit les dialogues). Il est important de bien référencer, ce que nous faisons ci-dessous.

FIGURE 2.8 – Mimi et Eunice – permission

— Œuvre originale : *Mimi and Eunice*, par Nina Paley, sur mimiandeunice.com [28].
— Source : publication en 2011, à l'adresse : `http://mimiandeunice.com/2011/08/30/permission-2/`.
— Traduction et modification par Framatophe.
— Licence : CC-BY-SA [29].

28. `http://mimiandeunice.com`
29. `https://creativecommons.org/licenses/by-sa/3.0/fr/`

CHAPITRE 3

Mes messages sur Internet

La communication est l'essence même d'Internet. Le réseau a été construit sur la base de protocoles de communication ouverts et accessibles à tous. Pour envoyer des messages, les utilisateurs peuvent utiliser plusieurs solutions logicielles. Dans ce chapitre, nous allons nous pencher sur les principaux usages : le courrier électronique et ses pratiques, les webmails, les clients de courriel, la messagerie instantanée et les principaux protocoles concernés. Nous aurons aussi l'occasion de toucher quelques questions de sécurité.

3.1 Le courrier électronique

« Vous avez reçu un courriel »[1]. Pour beaucoup, ce message est devenu très banal. Que ce soit dans un cadre professionnel ou personnel, l'envoi et la réception de courriers électroniques sont

1. Cette section est reprise en partie selon une section que l'auteur a rédigé dans le cadre d'un projet de Framabook intitulé *Guide de survie numérique.*

devenus des activités à part entière, comme planifier une réunion ou aller chercher son pain. Pour certaines personnes, les « méls » peuvent être rares voire inexistants, mais les institutions de l'État ou les acteurs économiques en général incitent de plus en plus à se passer de correspondance papier.

De manière commune, le courrier électronique se compare assez facilement à la lettre que l'on envoie via le service postal au coin de la rue. Cependant, le seul fait de communiquer par voie numérique implique des changements bien plus profonds. En effet, la comparaison avec la lettre sous enveloppe s'arrête là. Un courrier électronique est copié plusieurs fois sur les serveurs où il transite et tous les administrateurs de ces serveurs peuvent lire le courrier, un peu comme s'il s'agissait plutôt d'une carte postale. Si on veut une enveloppe, il faut *chiffrer* le contenu du courriel (voir la section consacrée au chiffrement). Faisons un petit tour des solutions de courrier électronique.

3.2 Les services de messagerie en ligne

Un service de messagerie en ligne est un service accessible via un navigateur Web. Une connexion est demandée, avec un nom d'utilisateur et un mot de passe.

Dans leur grande majorité, les services de courriel disposent d'une version en ligne, souvent appelée *webmail*, mais il est possible d'accéder à ses messages via un logiciel client de courriel (voir plus bas). On accède généralement à ces webmails sur le portail du fournisseur.

L'avantage d'un *webmail* est de pouvoir accéder à sa messagerie depuis n'importe quel ordinateur connecté. Parmi les nombreux services de messagerie en ligne, on peut distinguer les plus connus, qui mêlent à la fois un service d'émission et de réception de courriel, de la messagerie instantanée (*chat*), du stockage de fichiers en ligne, et des outils de réseaux sociaux. L'ensemble de ces services, accessibles depuis un compte unique, forme un *cloud (nuage)* où il

est possible de travailler sans avoir à stocker quoi que ce soit localement sur un ordinateur. Ajoutés à ce dispositif, on peut mentionner des systèmes d'édition de documents (bureautique) ou des systèmes de partage de fichiers images (photographies).

Tous ces services, accessibles via un seul compte, sont très révélateurs des usages personnels : partager facilement ses photos dans un cercle familial, ne plus avoir à trier ses courriels grâce à un espace de stockage quasi inépuisable pour la majorité des utilisateurs, pouvoir éditer à plusieurs des documents qui resteront stockés en ligne et accessibles à tout moment, etc.

Sur Internet, de grandes entreprises proposent de tels outils gratuitement, les mettant ainsi à disposition de millions d'utilisateurs à travers le monde. Les plus connues disposent souvent d'une version gratuite (imposant de la publicité en échange du service et des informations profilées des utilisateurs) et d'une version payante.

3.2.1 Mise en garde

Aussi séduisants qu'ils puissent être, les services de messagerie en ligne gratuits ou payants, sont souvent sous le feu des projecteurs. Ils supposent tous un certain degré de confiance de la part des utilisateurs qui acceptent des clauses de confidentialité parfois abusives, ou, plus simplement, ne remplissent pas leur devoir en matière de garantie de sécurité des données.

Si c'est gratuit, c'est vous le produit !

En particulier lorsque le service est gratuit, un utilisateur doit toujours être conscient qu'en déléguant à un tiers la gestion de son courrier personnel ou de n'importe quelles autres données, il s'engage à prendre le risque de les perdre ou de laisser à ce tiers la possibilité de les analyser pour en tirer des informations plus ou moins personnelles en vue d'une utilisation commerciale, ou pour le compte d'autrui (comme une agence de renseignements).

Par ailleurs, suivant les pays où sont stockées ces données (l'emplacement des serveurs), ces dernières ne sont plus forcément sous la même juridiction que l'émetteur ; là aussi des dispositions doivent être prises par les utilisateurs afin de se prémunir d'un éventuel défaut juridique ou d'un droit de regard exercé par un gouvernement mal intentionné.

3.2.2 Effacer mes traces

Les premières précautions à prendre lorsqu'on utilise un *webmail* est d'effacer ses traces une fois le travail terminé, tout particulièrement si la consultation a lieu depuis un cybercafé ou un ordinateur qui n'est pas à soi. En effet, puisqu'il est consulté depuis un navigateur, ce dernier conserve certaines données.

Il faut donc penser à :

— effacer l'historique de navigation et les cookies,
— ne pas accepter de stocker en mémoire les mots de passe et les champs de formulaires,
— penser à se déconnecter du service (clôturer la session de travail).

Pour cela un navigateur comme Firefox [2] propose des outils efficaces :

— utiliser le mode de navigation privée (menu `Fichier > Nouvelle fenêtre de navigation privée`),
— supprimer tout l'historique en une seule fois (Menu `Historique > Supprimer l'historique récent`, sélectionner la totalité de l'intervalle à effacer et cocher toutes les cases cookies, cache, préférences de site, etc.),
— installer des extensions pour limiter et monitorer la surveillance par cookies, tel Privacy Badger [3].

Enfin, tous les systèmes d'exploitation (GNU/Linux, MacOs, Windows, Android, etc.) permettent de se connecter avec un nom d'utilisateur et un mot de passe. Que vous utilisiez un ordinateur portable, une tablette ou un ordinateur fixe, il est primordial de ne pas laisser n'importe qui accéder à votre session et, donc, à tous

2. `https://www.mozilla.org/fr/firefox/new/`
3. `https://www.eff.org/fr/privacybadger`

vos documents, y compris le navigateur et son historique. Il ne faut donc pas hésiter à utiliser ce système supplémentaire de protection qu'est l'ouverture de session avec mot de passe.

3.2.3 Maîtriser mes connexions

La plupart des services en ligne, qu'il s'agisse de messagerie, de réseaux sociaux ou de stockage *cloud*, permettent de récupérer les mots de passe oubliés par une procédure basée sur l'envoi automatique d'un courriel. Bien que la procédure soit plus ou moins complexe selon le service concerné, il est important de ne pas négliger les étapes de sécurisation proposées lors de l'ouverture du compte :

— les phrases/questions secrètes,
— l'adresse courriel de secours (si possible),
— le niveau de complexité du mot/phrase de passe.

Concernant le mot de passe, deux erreurs courantes sont à éviter :

— utiliser le même mot de passe pour plusieurs voire tous les services en ligne utilisés,
— utiliser un mot de passe trop simple.

Se connecter en deux étapes

Certains services proposent une méthode dite de « validation en deux étapes » pour se connecter à sa boite aux lettres. Elle consiste par exemple, à chaque connexion, d'entrer d'une part le login et le mot de passe et, d'autre part, un code envoyé sur le téléphone portable servant à valider cette connexion. Cela nécessite de donner son numéro de téléphone portable à un tiers et d'avoir son téléphone à disposition lors de la connexion, mais elle complique efficacement toute tentative frauduleuse.

Reportez-vous au chapitre 5 pour de plus amples détails sur les mots de passe.

3.3 Les logiciels de messagerie (clients de courriel)

Un logiciel de messagerie est appelé un *client* de courrier électronique. Les *webmails* dont il vient d'être question à la section précédente en font partie. Ils sont reconnus comme étant des *clients légers*, parce qu'ils fonctionnent sur des serveurs en tant qu'applications accessibles à distance. Ils se distinguent des *clients lourds*, c'est à dire des logiciels qui s'installent localement sur un ordinateur et qui se chargent de récupérer les messages depuis un serveur de courriels.

Un client lourd : pourquoi utiliser un tel outil ?

— premièrement parce que vous n'êtes pas obligé-e d'être connecté-e en permanence. Si vous êtes en déplacement, sans connexion, vous pouvez toujours rédiger vos courriels, les sauvegarder et les envoyer une fois connecté-e ;
— en second lieu, vous pouvez configurer votre client de courriel comme *vous* le voulez. Par exemple vous pouvez utiliser un système de chiffrement à vous, tel GnuPG (cf. plus bas) ;
— enfin, vous pouvez gérer plusieurs comptes à la fois, en gardant la même interface. Vous pouvez même copier des messages d'un compte à l'autre, configurer vos dossiers, etc.

Le logiciel Mozilla Thunderbird [4] est sans doute l'un des plus connus. Il est distribué sous licence libre et sous ce nom depuis 2003, traduit dans plus de cinquante langues, et compatible avec les systèmes d'exploitation courants tels GNU/Linux, MacOS et Windows. Pour l'utiliser, vous devez déjà avoir une adresse courriel (vous pouvez la créer lors de la première ouverture du logiciel).

Au premier lancement du logiciel, ou lorsque vous souhaitez configurer un compte de messagerie, Thunderbird cherche à détecter automatiquement les protocoles de communication disponibles sur le serveur correspondant à votre adresse courriel. Ainsi, si vous avez entré une adresse du type `Jean.dupont@tictacmail.com`, Thunderbird tentera de se connecter au serveur de messagerie

4. `https://www.mozilla.org/fr/thunderbird/`

`tictacmail.com` et détectera les paramètres de connexion pour envoyer et recevoir du courrier, ainsi que les méthodes disponibles pour le faire (les protocoles).

Quelques explications s'imposent.

3.3.1 Configurer un client de courriel local

Pour envoyer et recevoir du courrier, il faut indiquer au logiciel de messagerie les informations qui lui permettront d'opérer :

— se connecter au serveur avec un nom de compte et un mot de passe,

— savoir avec quel protocole se connecter pour l'envoi et la réception, et gérer les messages en fonction de cette information.

De manière générale, pour configurer son logiciel de messagerie, vous pouvez vous satisfaire de la configuration qui vous est proposée par défaut. La plupart du temps le service de messagerie auquel vous êtes abonné-e diffuse dans ses pages d'aide toutes les informations nécessaires à la configuration d'un client de messagerie — adresse du serveur, protocoles disponibles, ports à configurer, ainsi :

— SMTP (*simple mail transfert protocol*) : utilisé pour le transfert du courrier électronique vers le serveur de messagerie. Le logiciel utilise le nom du compte et le mot de passe, soumet une requête au serveur et ce dernier reçoit le message.

— POP (*post office protocol*) : il est utilisé pour récupérer les messages depuis le serveur. Les messages sont alors *téléchargés*. Il est possible de configurer le logiciel de messagerie avec le protocole POP pour qu'il laisse ou non une copie des messages sur le serveur pendant une période déterminée.

— IMAP (*internet message access protocol*) : il est utilisé pour synchroniser les messages sur le serveur et sur le logiciel de messagerie. Autrement dit, il « laisse » les messages sur le serveur tant qu'on ne les supprime pas explicitement, il permet de travailler directement sur le serveur, de manipuler les messages et les dossiers.

— SSL (*secure sockets layer*) et TLS (*transport layer security*) : il s'agit de protocoles permettant de sécuriser les échanges sur internet. Ils ne concernent pas uniquement la messagerie, mais ils permettent de définir le niveau de sécurité avec lequel le logiciel peut se connecter au serveur pour l'envoi et la réception du courrier (et limiter ainsi toute possibilité d'interception).
— Les ports. Au moment de configurer votre client de messagerie, vous remarquerez certainement qu'à chaque protocole et son niveau de sécurité correspondent des ports logiques particuliers. Un port est à considérer comme une porte (c'est d'ailleurs son sens premier) empruntée par un programme informatique pour écouter ou émettre des informations. Pour l'envoi, par défaut le protocole SMTP émet sur le port 25. Mais si l'on souhaite sécuriser cet envoi avec SSL, il faut alors utiliser les ports 587 (ou parfois 465 selon le serveur de messagerie). Le protocole POP utilise le port 110 et de manière sécurisée le port 993. Le protocole IMAP utilise le port 143 et de manière sécurisée le port 993.

3.3.2 Exemple de configuration

Je dispose d'une adresse courriel `jean.dupont@youkoulele.fr` et je souhaite pouvoir utiliser ma messagerie en IMAP avec une connexion sécurisée.

Je me rends sur les pages de documentation de `youkoulele.fr` et j'apprends que pour configurer en IMAP, il me faut entrer ces informations pour une connexion SSL :

— IMAP port 993 serveur `mail.youkoulele.fr`
— SMTP port 587 serveur `mail.youkoulele.fr`

Lors de la configuration d'un nouveau compte avec l'assistant de Thunderbird :

Dans la page de gestion des comptes (`Édition > Paramètres des comptes`) :

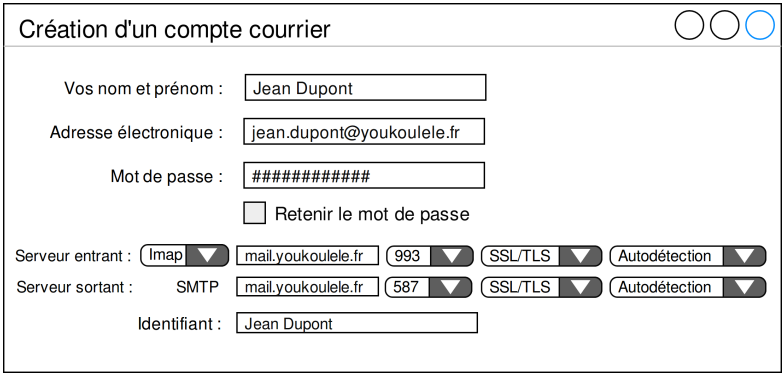


FIGURE 3.1 – Nouveau compte sur Thunderbird

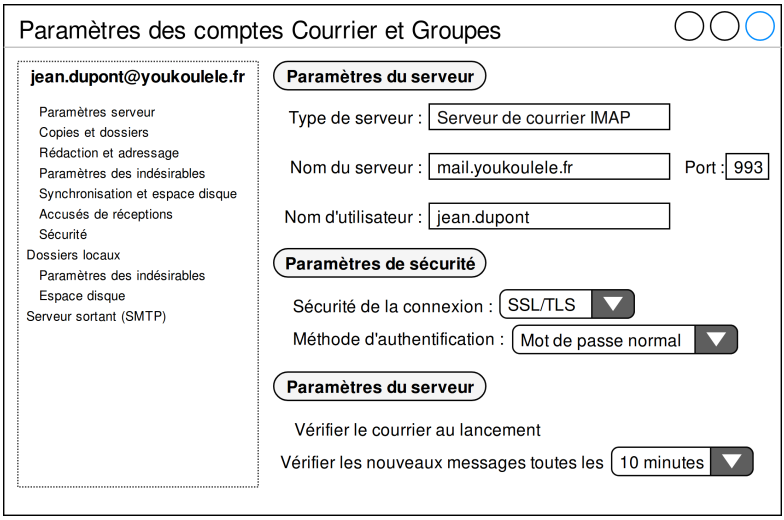


FIGURE 3.2 – Thunderbird : paramètres (1)

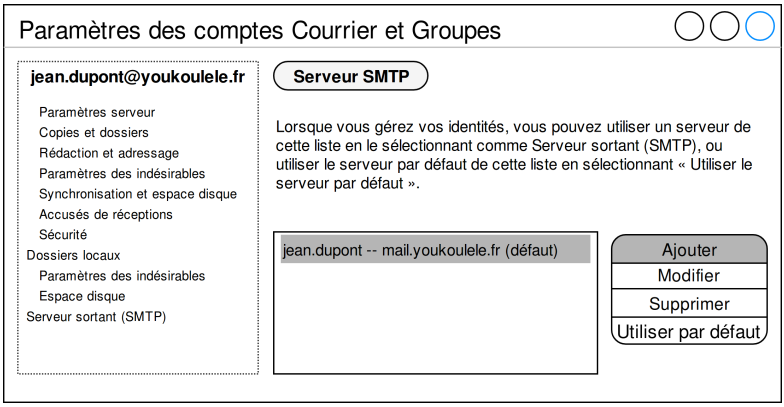


FIGURE 3.3 – Thunderbird : paramètres (2)

3.4 Les usages

Tout particulièrement lorsqu'il s'agit de communiquer via une messagerie électronique, il est primordial de respecter quelques règles d'usage. La Nétiquette constitue l'ensemble de ces règles informelles instituées en 1995, alors même qu'à l'arrivée d'Internet dans les foyers correspondait une multiplication exponentielle des communications par messagerie électronique, à titre individuel ou professionnel. Toutes les informations concernant la Nétiquette sont trouvables sur la page Wikipédia qui lui est consacrée (voir Nétiquette (Wikipédia) [5]). Nous résumerons ici quelques points importants concernant le courrier électronique.

3.4.1 Peaufiner la configuration de mon client de messagerie

Une fois entrées les informations permettant de recevoir et envoyer du courrier, quelques petites manipulations restent encore à faire.

5. http://fr.wikipedia.org/wiki/N%C3%A9tiquette

Dans la section consacrée aux options de rédaction des messages (dans Thunderbird, elle est nommée « rédaction et adressage », dans un *webmail* ces réglages sont accessibles via les options de votre compte), il est important de bien choisir la manière dont les messages seront rédigés.

— Utiliser le HTML pour envoyer un message vous permettra d'effectuer une mise en page sur votre contenu comme par exemple ajouter des couleurs, faire des effets de taille de caractères, etc. Néanmoins, si vous envoyez tous vos messages en HTML, c'est à dire comme une page web, soyez sûrs que votre correspondant pourra les lire dans la mise en page que vous avez souhaitée. Selon son logiciel et la manière dont il l'a configuré, cela ne sera peut-être pas le cas. De même, il n'est pas nécessaire d'envoyer un message en HTML accompagné de multiples images non pertinentes, comme une image de signature ou une image de fond de style « papier à lettre ». Il est donc souvent préférable de rédiger ses messages en mode texte brut (*plain text*).

— Lorsque qu'on répond à un message, il est de bon ton de commencer à l'écrire *en dessous* du message original. Cela est particulièrement utile lorsque le fil de discussion comporte plusieurs réponses : on peut alors suivre aisément le déroulé de la conversation de haut en bas. Ne pas hésiter, aussi, à supprimer les contenus non pertinents dans les messages précédent le vôtre, en particulier si vous répondez à un point précis de la discussion.

Une identité lisible

Il est préférable d'annoncer vos noms et prénoms dans les options qui concernent votre identité. Ainsi votre correspondant pourra lire votre adresse ainsi : `Jean Dupont <jean.dupont@youkoulele.fr>` au lieu de ne voir que votre adresse électronique. Ceci est particulièrement utile si votre adresse électronique ne reflète pas votre identité, comme `kikoo88@youkoulele.fr`, ce qui n'est pas conseillé sur un compte destiné à envoyer des correspondances officielles.

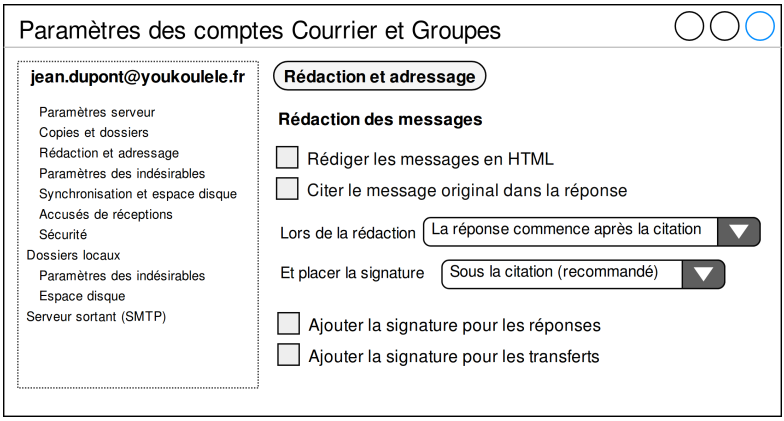


FIGURE 3.4 – Thunderbird : configuration de la messagerie (1)

3.4.2 Écrire mes messages

La Nétiquette citée plus haut vous permettra de retenir les pratiques courantes et les règles de respect en matière d'écriture de correspondance électronique. Néanmoins les quelques principes suivants sont toujours utiles à retenir.

Pour envoyer un courrier électronique, les champs suivants sont toujours demandés ou proposés :

— l'adresse ou les adresses du(es) destinataire(s) (champ `À:`),
— l'adresse ou les adresses du(es) destinataire(s) en copie (champ `Cc:`, copie carbone),
— l'adresse ou les adresses du(es) destinataire(s) en copie invisible (champ `Bcc:` ou `Cci`, Blind Carbon Copy, ou Copie Carbone Invisible),
— l'objet du message,
— le contenu du message.

Il faut savoir utiliser à bon escient les champs relatifs à la destination, en particulier la copie. La plupart du temps il est inutile d'envoyer le même message à une dizaine de personnes en supposant que, parce qu'elles reçoivent le message, elles le retiendront ou souhaitent obligatoirement le recevoir. Des pratiques non judicieuses sont souvent rencontrées dans les milieux professionnels

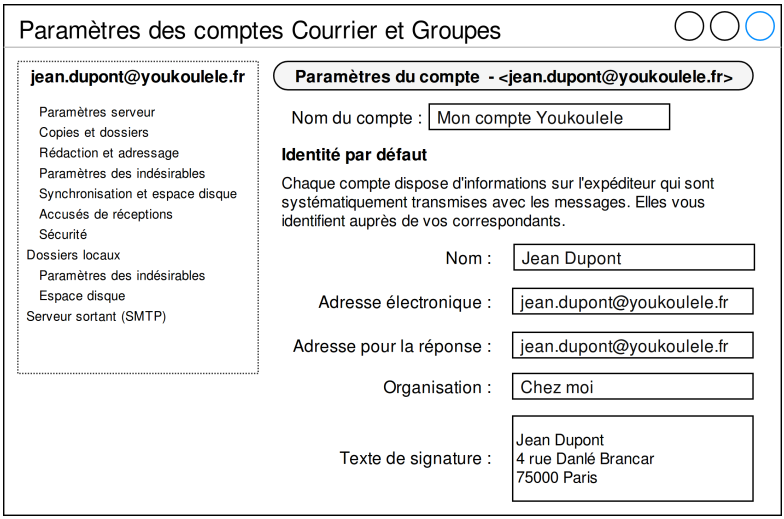


FIGURE 3.5 – Thunderbird : configuration de la messagerie (2)

où les messages collectifs génèrent du stress sous prétexte de dédouaner l'émetteur. Parfois, rien ne vaut un bon vieux coup de téléphone ou tout simplement parler autour d'un café, en passant.

La copie invisible est elle aussi à utiliser avec discernement. Parfois les non-dits peuvent être source de conflit, ou au contraire le choix des destinataires visibles et invisibles peut s'avérer diplomatique. Surtout, n'envoyez jamais un courriel à une liste de destinataires n'ayant aucun rapport entre eux sans utiliser la copie invisible : certains d'entre eux vous ont donné leur adresse courriel sans pour autant vous autoriser à la divulguer à des destinataires qui leurs sont inconnus !

L'objet du message, quant à lui, doit toujours refléter efficacement son contenu. Il permet au destinataire de classer ses messages et choisir le bon moment pour les lire. C'est l'objet qui détermine le fil de discussion. Si celle-ci dévie trop de son axe original, il devient judicieux de créer un nouveau courriel et définir un objet approprié pour créer un nouveau fil. Par facilité, ne faites pas une réponse à un courriel pour parler d'autre chose.

3.4.3 Les pièces jointes

Les pièces jointes sont les fichiers que l'on envoie à son destinataire en même temps que le message. Là aussi, quelques précautions d'usage s'imposent :

— s'assurer que le destinataire est bien en mesure de lire le fichier. Cela signifie qu'il faut garantir l'interopérabilité (voir chapitre 1) : ne pas supposer que le destinataire dispose du même logiciel que vous et dans sa même version. Par exemple, un document circulera mieux en version PDF que dans sa version originale issue d'un logiciel qui n'admet pas les standards ouverts.

— se demander si le fichier joint est vraiment utile : son contenu ne pourrait-il pas figurer directement dans le corps du message ? Ceci afin de ne pas obliger le destinataire à télécharger le fichier, l'ouvrir avec un logiciel, et faire plusieurs opérations superflues.

— si le fichier est uniquement destiné à un affichage sur écran, comme une photo par exemple, il est inutile de l'envoyer dans son format d'origine et en haute résolution. Compresser une image ne prend que quelques instants et facilite son chargement.

— avant d'envoyer un fichier à plusieurs destinataires, il faut se demander si tous les destinataires ont besoin de ce fichier, en particulier si l'espace disponible dans leur boîte à lettres est restreint.

— enfin, on pourra tout simplement se demander si l'envoi d'un fichier en pièce jointe ne serait pas mieux remplacé par un simple lien pointant vers ce même fichier stocké sur un serveur *cloud*. En effet, particulièrement lorsqu'il est volumineux, il est possible de stocker un fichier dans un espace de stockage en ligne et de le rendre accessible via une simple URL que l'on communique alors dans le message. Dans ce cas, les destinataires peuvent alors avoir le choix de télécharger ou non le fichier sans qu'il n'encombre leurs boîtes. L'association Framasoft propose par exemple deux

services permettant d'échanger des fichiers en toute confidentialité : Framapic [6] vous permet d'échanger une ou plusieurs images sous forme d'album, Framadrop [7] vous permet d'envoyer un fichier volumineux. Dans les deux cas, ce sont de simples liens que vous échangez par courriel.

3.5 Que dois-je savoir en plus ?

3.5.1 Chiffrement des messages

Il peut être parfois préférable d'envoyer des messages que seul le destinataire est capable de lire. Pour cela, la plupart des logiciels clients de courrier électronique disposent de fonctionnalités de chiffrement. La meilleure solution est basée sur GnuGPG (Gnu Privacy Guard), une implémentation libre de OpenPGP (Pretty good Privacy) et fonctionne via un système de clés privées et clés publiques (voir chapitre 5).

Pour utiliser ce système, certains logiciels clients disposent par défaut de tous les outils nécessaires pour configurer et gérer vos signatures numériques. Une extension connue pour Thunderbird se nomme *Enigmail*, et permet de chiffrer et déchiffrer les messages de manière automatique.

3.5.2 Bien choisir mon service de messagerie

Tout utilisateur disposant d'un abonnement auprès d'un fournisseur d'accès Internet dispose, pour ainsi dire « par défaut », d'un compte de messagerie dont le mot de passe est acquis en même temps que le contrat qui le lie à son fournisseur d'accès. Ce compte de messagerie est utile pour le fournisseur d'accès afin de communiquer avec son abonné. Cependant, rien n'oblige ce dernier à utiliser ce compte.

Plusieurs raisons peuvent justifier un autre choix : la qualité du service, certains protocoles (cf. ci-dessous) non accessibles pour

6. https://framapic.org/
7. https://framadrop.org/

l'abonnement contracté, manque de fonctionnalités, l'utilisateur dispose déjà d'une messagerie et ne tient pas à en changer en fonction de ses abonnements successifs, etc.

Plusieurs idées reçues doivent pourtant être combattues :

— croire qu'un service de messagerie doit être gratuit,
— croire que la gratuité n'engage à rien,
— penser que plus le service est connu, meilleur il est,
— ignorer que le choix d'un hébergement (pour sa messagerie ou autre chose) peut aussi être un choix de conviction.

Au moins deux principes doivent guider le choix d'un service :

— l'affichage clair de ses positions vis-à-vis de la sécurité et de la confidentialité des données que vous confiez,
— les fonctionnalités qu'ils propose et ce que l'on est éventuellement prêt à payer (ou sacrifier) pour cela.

Dans la mesure du possible, il est préférable d'évaluer la *fiabilité technique et éthique* du service, l'identité de l'entreprise ou de l'association qui le propose, et enfin, seulement, le coût éventuel.

Les exemples qui suivent concernent les Conditions Générales d'Utilisation (CGU) de trois acteurs spécialisés dans l'hébergement de services, dont le courrier électronique.

Extrait des CGU de l'association La Mère Zaclys (en date du 17/01/2017) :

> La Mère Zaclys est une association loi 1901 à but non lucratif qui propose des services en ligne tel qu'un album photos, un cloud, une boite email, un service de partage de fichiers et un lecteur de flux RSS. [...] Le site est hébergé sur des serveurs français (chez OVH à Roubaix), développé et maintenu sur le territoire français (Franche-comté) et utilise exclusivement des logiciels libres (linux). Le respect de votre liberté et de vos droits est pour nous une priorité absolue. Contrairement à d'autres sites bien connus, nous garantissons vos libertés et vos droits de propriété intellectuelle : La mère Zaclys ne s'accorde aucun droit d'utilisation, de reproduction, de modification, de création d'œuvres dérivées, de

> communication, de publication, de représentation, d'affichage, de distribution… de vos contenus. Votre contenu reste votre contenu et en aucun cas le nôtre.

Extrait des CGU de l'entreprise MailObject (Netcourrier) (en date du 17/01/2017) :

> L'entreprise MailObject, est une entreprise française ayant développé une technologie du même nom. Elle fournit un service baptisé Netcourrier (Net-C), en version gratuite (limitée) ou payante (avec plus de fonctionnalités), pour les particuliers, les familles ou les entreprises. Bien que proposant un service de stockage cloud, son activité se concentre sur le domaine de la messagerie. Elle revendique, via une charte [8] relative à la vie privée, son engagement pour une politique non intrusive et la défense des principes d'autonomie et de confidentialité.

Extraits des CGU de l'entreprise Google (en date du 17/01/2017) :

> Lorsque vous utilisez nos services ou que vous affichez des contenus fournis par Google, nous collectons et stockons des informations dans les fichiers journaux de nos serveurs. Cela comprend :
> — la façon dont vous avez utilisé le service concerné, telles que vos requêtes de recherche.
> — des données relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les données de routage des SMS et les types d'appels.
> — votre adresse IP.
> — des données relatives aux événements liés à l'appareil que vous utilisez, tels que plantages, activité du

> système, paramètres du matériel, type et langue de votre navigateur, date et heure de la requête et URL de provenance.
> — des cookies permettant d'identifier votre navigateur ou votre Compte Google de façon unique.
>
> [...] Lorsque vous utilisez des services Google, nous sommes susceptibles de collecter et traiter des données relatives à votre position exacte. [...] Lorsque vous contactez Google, nous conservons un enregistrement de votre communication afin de mieux résoudre les problèmes que vous rencontrez. [...] Nos systèmes automatisés analysent vos contenus (y compris les e-mails) afin de vous proposer des fonctionnalités personnalisées sur les produits, telles que des résultats de recherche personnalisés, des publicités sur mesure, et la détection de spams et de logiciels malveillants.

Les exemples qui précèdent illustrent des conceptions différentes d'une (ou plusieurs) proposition(s) de service(s). On comprend aisément que dans la mesure où ces données privées sont exploitées, et génèrent du bénéfice, le fournisseur peut offrir gratuitement et à l'échelle la plus large possible l'usage de ses services. Au contraire, dans le cas où ces données privées sont sanctuarisées par le fournisseur, faire payer le service est pour lui l'une des seules ressources pour pérenniser son activité. C'est en particulier le cas pour des associations qui, parce qu'elles bénéficient de l'engagement humain des bénévoles, proposent ce genre de services pour des coûts relativement bas visant à couvrir les frais d'infrastructure (reportez-vous au chapitre 4 où il est question du collectif CHATONS).

Les structures suivantes (tableau 3.1) sont des alternatives fiables et crédibles face aux « géants » les plus connus du web. Elles proposent des CGU respectueuses des données des utilisateurs. Certaines sont des entreprises, d'autres des structures sans but lucratif. Toutes font reposer leurs services sur des solutions de

logiciels libres. Consultez leurs CGU et prenez l'habitude de procéder ainsi pour choisir votre fournisseur de service, en connaissance de cause. Bien sûr, un fournisseur pourra toujours changer ces CGU, voire ne pas les respecter. Par ailleurs, n'oubliez jamais qu'à moins d'héberger vous même votre messagerie, vous devez faire confiance à un tiers. En la matière, la transparence est donc nécessaire.

Nom	Webmail	imap, pop, smtp, ssl	Chiffrement
mail.zaclys.com	X	X	X
riseup.net	X	X	X
ouvaton.coop	X	X	X
lautre.net	X	X	X
infini.fr	X	X	X
mailoo.org	X	X	X
netcourrier.com	X	X	X X
mailfence.com	X	X	X X X
protonmail.com	X	N	X X X

TABLEAU 3.1 – Quelques fournisseurs de messagerie. Certains proprosent aussi les protocoles Exchange/ActiveSync (Microsoft)

3.5.3 Héberger mon propre serveur courriel

Nous ne saurions terminer cette section sans mentionner l'autohébergement de son propre serveur de messagerie. Cette possibilité est réservée à des utilisateurs avancés et tout particulièrement attentifs aux questions de sécurité (car il faut alors assumer seul la protection de ses données). Mais peut-être autour de vous des personnes peuvent prendre en charge un tel serveur, pour le compte de la famille, d'un groupe, d'une association.

En effet, pour envoyer et recevoir des courriers électroniques, il n'y a aucune obligation de stocker ses messages auprès d'un service tiers : cela est possible chez soi, sur un ordinateur configuré pour cela, ou sur un serveur distant loué à cette occasion (ce qui revient à utiliser un service tiers mais en gardant la main sur les solutions logicielles utilisées).

De nombreux tutoriels sont présents sur la toile, et montrent comment configurer *postfix* ou *sendmail*, des logiciels libres permettant de gérer un service de messagerie. Par ailleurs, les facilités se sont récemment multipliées. On peut mentionner par exemple le marché des *nano-computers*, des mini ordinateurs consommant très peu d'énergie et vendus à très bas prix, permettant justement de mettre en place un serveur chez soi sans mobiliser une grosse machine pour cela. Enfin des systèmes de gestion de serveur permettent de faciliter la configuration des logiciels utilisés pour obtenir des solutions fiables et basées sur des logiciels libres. On peut citer Yunohost [9] et Cozy Cloud [10], qui permettent bien plus qu'un serveur de courriel.

3.5.4 Mes courriels avec un smartphone

Par défaut, les smartphones embarquent des applications de gestion de courrier électronique. Pour les systèmes Android, il y a la plupart du temps installés d'emblée le client de courriel choisi par le fabricant et l'application Gmail. Les deux permettent de se connecter à un serveur de son choix, y compris avec différents protocoles (pop, imap, exchange, etc.), et de rapatrier son courriel. Or, les interfaces proposées peuvent ne pas vous convenir, mais surtout vous ne maîtrisez pas la manière dont ces courrielleurs se connectent à votre boite à courriel.

Des enquêtes approfondies montrent régulièrement les failles de ces clients de courriel sur appareils mobiles. Parfois, plus que de simples failles de sécurité, ce sont de véritables intrusions dont il s'agit, comme le montre Charly dans une étude technique [11] mais néanmoins vulgarisée. L'étude de Charly concerne deux applications connues qui ne se contentent pas de rapatrier le courriel. En réalité, elles s'approprient et envoient vos login et mot de passe sur les serveurs du fournisseur de l'application et correspondent alors directement avec les serveurs de vos courriels, qu'il s'agisse

9. `https://yunohost.org/#/`
10. `https://cozy.io/fr/`
11. `http://linuxfr.org/users/charlycha/journaux/mefiez-vous-des-applications-de-courriel-sur-mobile`

de votre boîte mail personnelle ou celle de votre entreprise. En d'autres termes : n'utilisez pas et n'installez pas n'importe quel client de courriel sur votre mobile !

L'application libre K9-Mail [12] fait toutefois office de référence en la matière et bénéficie d'un développement très actif. On peut dire que K9-Mail s'utilise et se configure comme un client sur ordinateur. Si vous avez lu ci-dessus l'exemple de configuration de Thunderbird, vous pouvez reproduire la méthode avec K9-Mail, en plus de plein d'autres options. Par ailleurs, K9-Mail intègre une autre application, OpenKeyCHain [13], qui permet d'utiliser PGP pour chiffrer ses communications (cf. le chapitre 5).

3.6 La messagerie instantanée

On appelle messagerie instantanée une forme de dialogue en ligne, autrement nommé *chat* (anglicisme francisé en *tchat*). Il se pratique par l'intermédiaire de terminaux (ordinateur fixe, smartphone, tablette) connectés au même réseau. La messagerie instantanée se pratique à l'aide d'un logiciel client connecté à un serveur. Le logiciel peut être un client installé localement sur votre machine ou bien sous forme d'un service web, comme par exemple Gtalk intégré dans les services de Google.

Comme c'est le cas pour le courriel, les services de messagerie instantanée utilisent des protocoles particuliers. Certains sont des protocoles fermés, c'est le cas de Microsoft Messenger ou Yahoo !Messenger. Leur principal défaut est de maintenir les utilisateurs sur les réseaux qui utilisent ces protocoles avec l'impossibilité de pouvoir discuter avec des utilisateurs utilisant d'autres protocoles. On dit alors qu'ils sont *non-interopérables*.

Un autre défaut est relatif à la sécurité : en tant que systèmes fermés, seule la confiance que vous avez envers le fournisseur du service vous permet de mesurer le degré de confiance que vous pouvez accorder pour transmettre des informations (texte, vidéo,

12. `https://k9mail.github.io/`
13. `https://www.openkeychain.org/`

audio) à travers ces réseaux. Dans la mesure où la confiance numérique nécessite une expertise, il vaut mieux se tourner vers des standards ouverts, qui, eux, bénéficient de l'expertise de leurs utilisateurs.

Ces systèmes fermés ont eu leurs heures de gloire à l'époque où les alternatives utilisant des standards ouverts ne pouvaient pas encore assurer toutes les fonctionnalités offertes par ces systèmes propriétaires, comme par exemple le vidéo-chat. Aujourd'hui, certains standards comme XMPP permettent de faire des discussions privées et de salon, supportent la vidéo et l'audio, et utilisent des protocoles de sécurité sérieux. Pour ce qui suit, nous allons nous pencher sur l'un des plus connus : XMPP.

3.6.1 Utiliser XMPP

Le protocole XMPP [14] (Extensible Messaging and Presence Protocol) est en fait un ensemble de protocoles dédié à l'échange en ligne (instantané ou non). Le standard ouvert XMPP a été déployé par l'Internet Engineering Task Force (IETF) sur la base de la reconnaissance du protocole Jabber, créé par Jérémie Miller. L'intérêt de Jabber / XMPP était double :

1. proposer une plate-forme de serveurs de messagerie instantanée capable de communiquer de manière transparente avec tous les autres systèmes de messagerie (d'où l'intérêt de placer ce système sous licence libre pour que les autres acteurs puissent s'en emparer),
2. créer un système *décentralisé*, c'est-à-dire permettre aux utilisateurs de créer un compte sur n'importe quel serveur XMPP et pouvoir communiquer avec tous les comptes situés sur n'importe quel serveur (à la différence des comptes comme Skype qui nécessitent d'avoir un compte sur un serveur en particulier).

L'avantage est que si un serveur tombe ou se trouve censuré (ce qui peut arriver dans une dictature par exemple), cela n'empêche par pour autant les échanges avec XMPP. Alors que si Microsoft

14. `https://xmpp.org`

décide d'arrêter ses serveurs Skype, plus aucun compte ne pourra communiquer.

To be or not to be

De nombreux acteurs industriels ou de services utilisent désormais XMPP et le proposent aux utilisateurs. Il est possible, par exemple avec un compte Gtalk de communiquer via XMPP. Facebook, en revanche, après avoir ouvert temporairement l'accès à XMPP, a décidé de le fermer en 2015, obligeant ainsi ses utilisateurs à utiliser exclusivement l'application de Facebook.

Pour utiliser XMPP l'idéal est de trouver un logiciel client qui permet de créer un compte et de l'utiliser d'emblée. Pour cela vous pouvez choisir Pidgin [15], qui a aussi l'avantage de proposer beaucoup d'autres protocoles (y compris non libres) et de regrouper ainsi tous vos comptes de messagerie instantanée.

Après avoir installé Pidgin, créez un nouveau compte et choisissez le protocole à utiliser. Dans l'illustration suivante, le choix porte sur XMPP.

Choisissez ensuite un nom d'utilisateur et un *domaine*, c'est-à-dire le serveur Jabber/XMPP sur lequel vous avez un compte. Si tel n'est pas le cas, vous pouvez cocher en bas la case `Créer ce nouveau compte sur le serveur`.

Si vous ne connaissez pas de serveur, vous pouvez choisir l'un de ceux proposés sur la liste des serveurs publics [16]. Par exemple : le serveur de l'Apinc [17] ou celui de La Quadrature du Net [18].

Ensuite, si seulement vous en avez besoin, et selon les spécifications expliquées sur la page du serveur que vous choisissez (par défaut ne faites rien), allez dans l'onglet `Avancé` et choisissez la méthode de chiffrement, le port et le proxy si besoin.

15. `https://www.pidgin.im/`
16. `https://xmpp.net/directory.php`
17. `https://jabber.apinc.org/`
18. `https://jabber.lqdn.fr/`

FIGURE 3.6 – Configuration de Pidgin pour utiliser XMPP

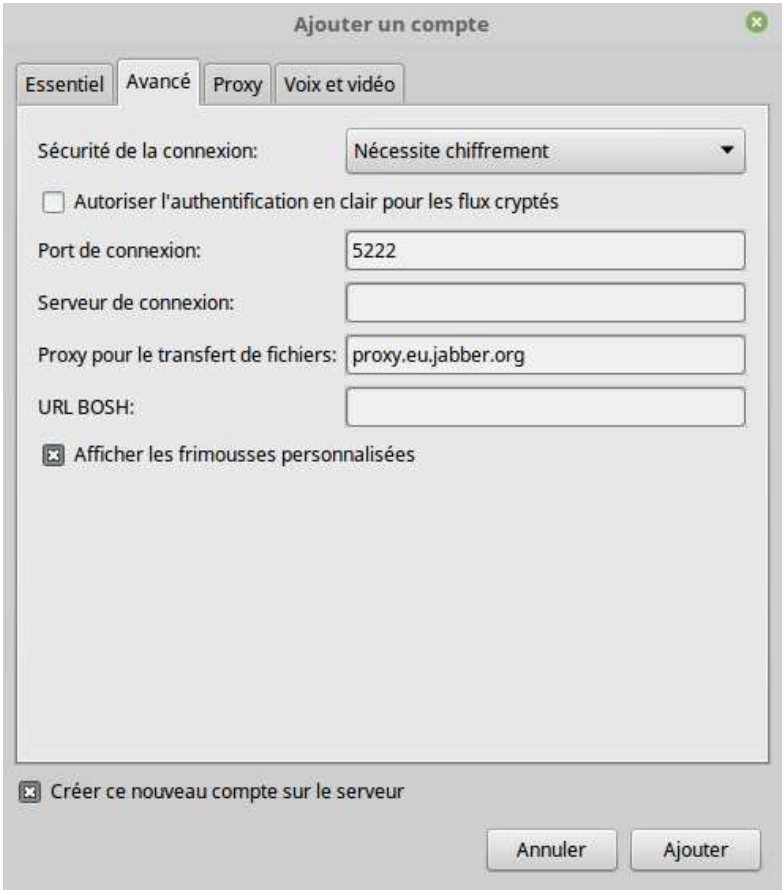


FIGURE 3.7 – Configuration avancée de Pidgin

3.6.2 Maîtriser ma messagerie instantanée

De nombreuses extensions sont disponibles pour Pidgin. Elles sont listées sur la page wiki du site officiel [19]. Pour une communication utilisant le chiffrement puissant de type OTR (Off-the Record Messaging), il faut installer le plugin *Pidgin-otr* (sur votre poste comme celui du correspondant). Pour comprendre comment procéder, vous pouvez suivre ce tutoriel [20].

La messagerie instantanée n'est pas réservée aux postes fixes. Sur tablette ou smartphone, il est aussi intéressant de pouvoir disposer d'outils qui permettent de communiquer rapidement et en toute sécurité.

L'application Xabber [21], par exemple, est un logiciel libre utilisant le protocole XMPP et permet de chiffrer facilement ses conversations avec OTR. Xabber permet aussi de se connecter à un compte Gtalk. La configuration du compte diffère très légèrement de Pidgin.

Dans le champ `Identifiant` entrez `votrelogin @nomduserveur.xx`. Votre serveur est le serveur sur lequel vous avez déjà un compte ou bien, si vous n'y avez pas encore de compte, vous pouvez le créer d'emblée en cochant la case `Créer un nouveau compte`. Si vous activez OTR pour ce compte, vous serez invité à installer un second logiciel nommé Orbot [22], si cela n'est pas déjà fait. Il s'agit de l'application TOR pour smartphone.

On peut noter que, en matière de messagerie instantanée sur plate-forme mobile, l'une des applications les plus sécurisées n'utilise pas XMPP. Elle a pour nom Signal [23], un logiciel libre développé par Open Whisper Systems. Signal utilise un protocole cryptographique justement nommé Signal, qui assure un chiffrement de bout en bout : seuls les utilisateurs de Signal peuvent lire leurs messages chiffrés. Pour l'utiliser, il faut donc que les correspondants disposent de la même application. Signal assure aussi de la VoIP (le

19. `https://developer.pidgin.im/wiki/ThirdPartyPlugins`
20. `https://securityinabox.org/fr/guide/pidgin/windows/`
21. `https://www.xabber.com/`
22. `https://guardianproject.info/apps/orbot/`
23. `https://whispersystems.org`

téléphone via Internet), toujours de manière chiffrée avec le protocole ZRTP [24]. Un client Signal pour ordinateur est aussi disponible, il se nomme Signal Desktop [25] et fonctionne en tant qu'extension à Google Chrome.

Si vous voulez utiliser de la VoIP en utilisant XMPP (et donc votre compte) vous pouvez utiliser l'application Jitsi [26], un client développé par l'Université de Strasbourg. Vous pouvez ainsi faire de la téléphonie IP depuis votre mobile ou votre ordinateur. Comme Pidgin pour le tchat, Jitsi est aussi ouvert à d'autres protocoles libres ou non.

24. https://fr.wikipedia.org/wiki/ZRTP
25. https://whispersystems.org/blog/signal-desktop/
26. https://jitsi.org/

CHAPITRE 4

Réseaux sociaux et hébergement

Un hébergement web est d'abord une prestation de service. Il s'agit de mettre à disposition des serveurs afin que les utilisateurs puissent y stocker des données accessibles en tout temps (tant que le serveur fonctionne). La première forme d'hébergement couramment rencontrée est l'hébergement de site web : un serveur doté d'une configuration spécifique (serveur HTTP, système de gestion de base de données, etc.) permet à l'utilisateur d'ouvrir un compte, et stocker des fichiers permettant de créer un site publiquement accessible. Par exemple, le premier site web était hébergé sur un serveur du CERN (où furent inventées les fonctions hypertexte du World Wide Web) à la fin des années 1990 [1].

Mais aujourd'hui, la transformation des technologies web et l'accroissement de l'offre ont fait de l'hébergement un vaste marché économique. Des entreprises font héberger leurs données sensibles, car il est parfois plus intéressant de ne pas s'occuper soi-même de la sécurité de ses données et laisser le soin à d'autres professionnels

1. On peut se reporter au site internet du CERN (Conseil européen pour la recherche nucléaire,) qui contient une rubrique dédiée « La naissance du web [2] ».

de le faire. Des hébergeurs de sites web professionnels font payer des individus ou des entreprises pour monter leurs blogs ou leur vitrines de vente en ligne. Certains hébergements sont spécialisés dans le stockage de données à distances, d'autres sont spécialisés en plate-forme de blog, d'autres encore dans la gestion de base de données distantes, etc. Certaines formes d'hébergement sont gratuites ou offrent des fonctionnalités et en font payer d'autres (ce qu'on appelle les offres premium). Enfin, des hébergeurs libres et associatifs existent et, moyennant une adhésion, proposent des services web plus ouverts.

Si vous voulez avoir votre profil sur un réseau social, héberger vos données, ouvrir votre blog personnel, partager vos photos et autres documents, synchroniser vos contacts ou vos notes personnelles tout en les partageant ou non… il est assez difficile de s'y retrouver dans toute l'offre disponible. En fait, il est surtout difficile de ne pas céder aux sirènes des solutions gratuites proposées par des grandes firmes dont on peut questionner les véritables intentions. Nous allons tenter dans ce chapitre d'y voir plus clair.

4.1 Connaître mes réseaux sociaux

Les services de réseaux sociaux, tout comme les services de messagerie (cf. le chapitre 3), sont des services d'hébergement. Dans le cas d'un hébergement de messagerie, vos courriels sont envoyés et copiés sur un serveur, relayés sur un autre serveur de réception et sur le terminal de votre correspondant lorsqu'il se connecte. Sur un service de réseau social classique (car nous verrons qu'il existe des alternatives) vous envoyez et copiez des contenus sur un serveur et ces contenus seront accessibles pour qui se connecte au même serveur.

Il existe plusieurs sortes de services de réseaux sociaux : Facebook, Google+ et LinkedIn sont des réseaux relationnels, Instagram un réseau pour photos et images, Youtube et Periscope sont spécialisés dans la vidéo… Tous ces services ont en commun le fait de centraliser les données et les connexions de manière à rendre

captifs les internautes et générer une économie de l'attention en insérant des publicités, en analysant les comportements et en investissant par ailleurs sur des produits en lien avec ces comportements (comme par exemple des applications pour mobile ou des voitures sans chauffeur).

Préférez des réseaux décentralisés

Le problème de la centralisation des réseaux sociaux, c'est la possibilité que leur accès soit compromis. Ce fut le cas par exemple en Égypte lors des manifestations populaires en hiver 2011 contre le gouvernement de Hosni Moubarak : les accès aux réseaux sociaux furent coupés par les autorités de manière à empêcher les relais d'appels à manifestations. Alors que les réseaux sociaux peuvent être d'excellents outils démocratiques, la centralisation des accès en est le talon d'Achille.

Un autre souci lié à l'usage de certains réseaux sociaux est la surveillance systématique des échanges. Si cette surveillance ne s'apparentait qu'à une analyse des contenus dans un but purement commercial, on pourrait à la rigueur considérer que les utilisateurs agissent en connaissance de cause et que, si leurs intimités numériques viennent à devenir publiques ou prises en otage par piratage, c'est leur responsabilité qui serait tout autant en jeu que celle du fournisseur de service. Hélas, ce n'est pas le cas. Comme le rapportent régulièrement les enquêtes journalistiques, des programmes de surveillance scannent *tous* les échanges, y compris privés, en vue d'identifier ceux qui présentent éventuellement des risques sécuritaires : c'est le cas notamment de Facebook, pour qui fut identifié en 2012 un programme interne de surveillance (c'est-à-dire qui relève de la propre initiative de Facebook). Officiellement ce programme servait à identifier les risques terroristes, les réseaux pédophiles, etc., de manière à redorer le blason de Facebook auprès des autorités. Mais quelle société démocratique est prête à voir tout son courrier ouvert et lu au nom de la surveillance sécuritaire, pour

sauvegarder les intérêts d'une firme privée ou même pour la raison d'État ?

Si vous désirez utiliser un service de réseau social, posez-vous donc la question de savoir ce que vous êtes prêt à sacrifier pour cela. Si la démocratie, la liberté d'expression et votre intimité sont importants à vos yeux, il est vivement encouragé d'étudier quelques alternatives aux réseaux centralisés. En voici quelques unes.

4.1.1 Diaspora*

Que faut-il pour qu'un réseau ne soit jamais coupé ? Il faut que chacun de ses nœuds soit relié à tous les autres et que chaque nœud fasse passer l'information indifféremment vers l'un ou l'autre de ses semblables (ses pairs). Imaginons qu'un logiciel de réseau social soit installé sur chacun de ces nœuds : vous obtenez Diaspora*, c'est-à-dire un réseau social constitué de multiples instances interconnectées.

Vous vous inscrivez sur une instance de votre choix et tous les membres des autres instances peuvent lire votre billet (si vous l'avez rendu public). Chaque instance peut avoir des conditions d'utilisation différentes, mais quoi qu'il en soit, vous pouvez communiquer entre tous les membres du réseau.

Ainsi Diaspora* est une alternative sérieuse et complète par rapport à un service comme Facebook. Par ailleurs des passerelles permettent de poster un billet sur Diaspora* et de le relayer automatiquement sur Facebook ou Twitter. Concernant les profils, ceux-ci sont chiffrés : faire d'un autre abonné un « ami » consiste à lui fournir une clé de chiffrement PGP (cf. le chapitre 5) lui permettant de déchiffrer votre profil privé ou vos messages privés. En d'autres termes, Diaspora* est un réseau social libre, décentralisé et sécurisé. Pour choisir un nœud (*pod*) Diaspora où vous pouvez vous inscrire et commencer à partager des contenus, rendez-vous

sur la liste Poduptime [3]. Par exemple, le *pod* maintenu par l'association Framasoft se nomme Framasphère, accessible sur framasphere.org [4] et regroupe beaucoup d'utilisateurs.

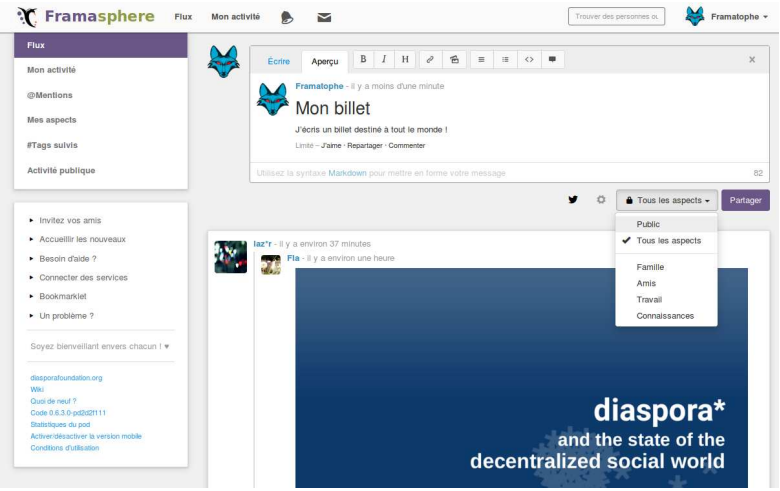


FIGURE 4.1 – Framasphère est un nœud Diaspora*

4.1.2 Movim

Movim est un réseau social décentralisé basé sur les mêmes principes que Diaspora* mais utilisant une technologie différente : le protocole XMPP (nous en parlons dans le chapitre 3). La force de Movim est d'avoir réussi à donner une dimension web à un protocole de messagerie. Ainsi, si vous disposez d'un compte Jabber/XMPP (très facile d'en créer un !), vous pouvez aussi vous connecter à Movim en utilisant les mêmes identifiants. Une autre solution consiste à choisir un nœud sur le site movim.eu [5].

3. `https://podupti.me/`
4. `https://framasphere.org/`
5. `https://movim.eu/`

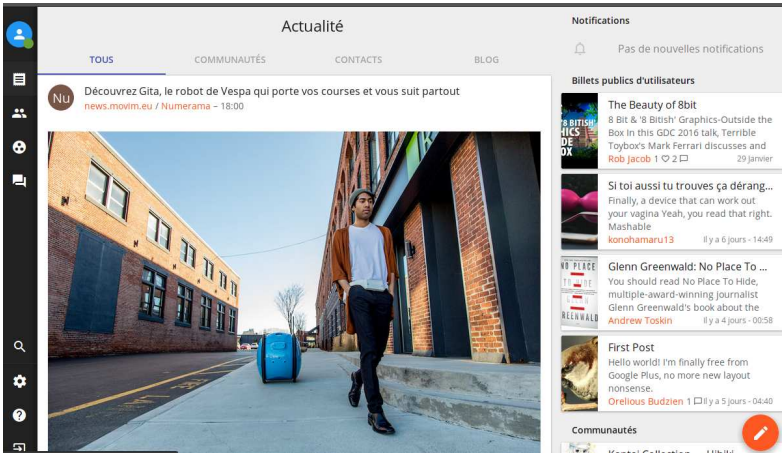


FIGURE 4.2 – Un mur sur Movim

4.1.3 Seenthis

Seenthis (accessible sur seenthis.net[6]) est un service de micro-blogging, c'est à dire qu'il permet des publications courtes ou très courtes, mais néanmoins plus longues que ce que permet Twitter. Seenthis se revendique être une plate-forme de *short-blogging*, spécialisée dans la publication de textes très courts, de liens, d'images avec une légende, etc. Chaque billet peut aussi être commenté par les lecteurs. Par ailleurs, Seenthis ne vise pas à remplacer Twitter : des ponts existent entre les deux services et l'on peut émettre vers Twitter tout en postant un billet sur Seenthis. Là où Seenthis constitue une alternative, c'est pour deux raisons :

1. Le code source est disponible[7], ce qui implique que le logiciel peut être installé ailleurs et être fréquenté par une autre communauté. Ainsi, par exemple Les Amis du Monde Diplomatique ont une plate-forme Seenthis, nommée Zinc[8], qui leur est dédiée (mais tout le monde peut s'y inscrire). Néanmoins, Seenthis n'est pas un réseau décentralisé comme Diaspora*

6. https://seenthis.net
7. https://github.com/seenthis/seenthis
8. http://zinc.mondediplo.net/

car il n'y a pas de correspondance entre différentes instances de Seenthis. Ainsi, une instance de Seenthis reste un réseau centralisé pour la communauté qui la fréquente.

2. Les conditions d'utilisation de Seenthis [9] (sur seenthis.net [10]) engagent le service à ne revendiquer aucun droit sur les billets publiés qui restent propriété de leurs auteurs, libres de les éditer ou les récupérer par la suite ou encore d'y apposer une licence libre.

FIGURE 4.3 – Auteurs et thèmes suivis sur Seenthis

4.1.4 Mastodon

Enfin, il faut signaler Mastodon [11], qui est à la fois un réseau social et une plate-forme de micro-blogage. Décentralisé à l'image de Diaspora*, il permet d'écrire des mini-billets (de 500 caractères

9. https://seenthis.net/fran%C3%A7ais/mentions/article/propri%C3%A9t%C3%A9-intellectuelle
10. https://seenthis.net
11. https://joinmastodon.org/

maximum). Le réseau Mastodon est constitué de multiples instances, dont les inscriptions sont ouvertes, d'autres qui ne le sont pas. Chaque instance propose ses propres conditions d'utilisation, dont il est conseillé de prendre connaissance avant de s'inscrire. Une fois connecté, l'utilisateur peut choisir différents canaux : ses propres abonnements, le canal de l'instance locale, le canal général (transversal). Des applications mobiles pour Mastodon existent, tels Tusky pour Android et Amaroq pour iOS.

En 2017, soit à peine un an après sa création, Mastodon regroupe des milliers d'utilisateurs, dont beaucoup ont déserté Twitter, préférant migrer vers cette solution libre. L'originalité de Mastodon est de permettre la naissance d'instances dont on choisi le degré d'ouverture au reste du réseau. Par exemple, une entreprise peut très bien installer Mastodon uniquement pour un usage interne, ou bien ouvrir son instance mais n'autoriser les inscriptions que pour ses membres.

On peut noter que la DINSIC (la Direction interministérielle du numérique et du système d'information et de communication) a ouvert sa propre instance Mastodon [12], destinée aux agents publics de l'État Français, un cas d'usage assez rare pour être souligné. Framasoft a ouvert l'une des plus importantes instances francophones, nommée Framapiaf [13], de même pour le magazine Numérama [14], La Quadrature du net [15], et bien d'autres.

4.2 Le cloud

Le *cloud computing* ou l'informatique en nuage consiste à utiliser les capacités de serveurs distants en passant par le réseau. Le principe est déjà très ancien ! C'était le but des premiers ordinateurs que de servir de ressources centrales. Les gros ordinateurs *mainframe* qui furent construits dès les années 1950 accomplirent

12. `https://mastodon.etalab.gouv.fr`
13. `https://framapiaf.org`
14. `https://social.numerama.com`
15. `https://mamot.fr/`

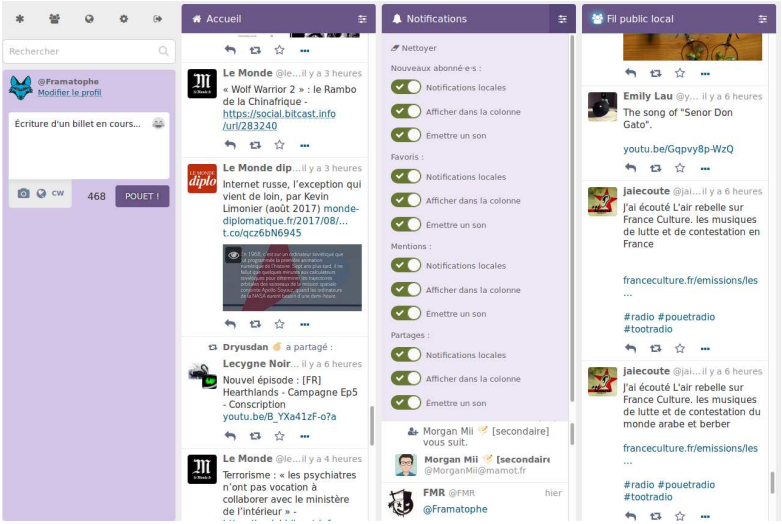


FIGURE 4.4 – Instance Framapiaf pour Mastodon

essentiellement ce rôle, de plus en plus avec le réseau Internet naissant à la fin des années 1960, mais en perte de vitesse avec l'apparition de l'informatique personnelle dans les années 1980. Ces ordinateurs étaient dotés d'une particularité : ils avaient un système d'exploitation à *temps partagé*, c'est-à-dire que plusieurs utilisateurs (notamment, à cette époque, des instituts de recherche, des banques, des ingénieurs aéronautiques…) pouvaient se connecter simultanément et effectuer des opérations en profitant du temps de calcul disponible. C'est l'une des caractéristiques qui a fait le succès du système Multics (Multiplexed Information and Computing Service), qui deviendra Unix plus tard.

Aujourd'hui, il existe un *cloud computing* destiné au grand public [16]. Il consiste essentiellement à :

16. Une autre application moins connue, consiste à faire du temps partagé « à l'envers », c'est-à-dire profiter des capacités de calcul des ordinateurs personnels pour centraliser ensuite les résultats. C'est l'exemple de BOINC [17] (Berkeley Open Infrastructure for Network Computing), une plate-forme de calcul distribué : les utilisateurs installent sur leur ordinateur un petit programme qui tourne en tâche de fond lorsque l'ordinateur est peu ou pas utilisé. Cela crée un potentiel de puissance

— héberger des fichiers (documents, photos, vidéos…),
— utiliser des logiciels en ligne (traitement de texte, espaces collaboratifs…),
— synchroniser des bases de données (des contacts, agendas…).

FIGURE 4.5 – IBM System/360 au Computer History Museum. Wikipedia Commons. Erik Pitti. CC-By

4.3 Enjeux de sécurité

Si vous choisissez de stocker des données à distance, que ce soit pour effectuer des sauvegardes ou pour partager des fichiers, cela implique d'évaluer le niveau de confiance que vous êtes prêt à accorder à un tiers. Dans le chapitre 5 nous expliquons qu'il est parfois souhaitable de chiffrer ses fichiers, notamment avec PGP. Lorsque vous stockez des fichiers sur l'ordinateur d'un tiers, vous

de calcul énorme qui peut alors être mis à disposition de la recherche dans différents domaines (médecine, astrophysique, mathématiques…).

avez tout intérêt à les chiffrer, au moins pour que personne d'autre que vous ne puisse les lire.

L'exemple du service Dropbox illustre bien le problème du stockage de données personnelles à grande échelle. En vrac :

— en janvier 2017, des utilisateurs s'aperçoivent que des fichiers supprimés depuis longtemps réapparaissent, ce qui sous-entend que même si l'utilisateur décide de supprimer des données, Dropbox les conserve [18] ;
— en été 2016, Dropbox demande à ses abonnés de changer de mot de passe : des pirates ont réussi à exploiter une faille connue depuis 2012 et 68 millions de comptes (deux tiers des utilisateurs) ont ainsi vu leurs identifiants piratés [20] ;
— au printemps 2016, Dropbox sort une nouvelle version dont l'application locale s'immisce dans le système d'exploitation des utilisateurs au risque de créer de graves failles de sécurité [22].

Il faut considérer que les difficultés rencontrées par le service Dropbox ne sont pas extraordinaires. Leurs conséquences, en revanche, sont particulièrement problématiques : en créant un immense silo de données pour des millions d'utilisateurs, un tel service s'expose naturellement à un taux élevé de risque d'erreur et à moult convoitises. Dans ces conditions, centraliser toujours plus de données et créer un monopole n'est pas un facteur de confiance.

D'un autre côté, choisir un hébergeur associatif ou autohéberger ses données implique aussi des risques (que l'association soit dissoute, que les mesures de sécurité ne soient pas d'un niveau suffisant, etc.) , mais ils seront d'autant moindres que la structure à laquelle on accorde sa confiance reste assez proche de ses utilisateurs pour leur garantir l'effort et le conseil. Quant à l'autohébergement, il est sage de prendre la mesure de ses propres compétences.

18. Voir Gabriele Porrometo, « Dropbox justifie la soudaine réapparition de fichiers supprimés sans vraiment convaincre [19] », *Numerama*, 27/01/2017.

20. Voir Guillaume Serries, « Dropbox : 68 millions d'identifiants dans la nature, mais tout va bien [21] », *ZDNet*, 31/08/2016.

22. Voir Christophe Lagane, « Le nouveau Dropbox, une menace pour la sécurité ? [23] », *Silicon.fr*, 30/05/2016.

4.4 Quels services choisir ?

Avant de choisir un service dans les nuages, il faut réfléchir à l'usage que l'on souhaite en faire. S'il s'agit par exemple de prendre quelques notes, un service d'édition de documents en ligne ne sera pas pertinent. S'il s'agit de partager les dernières photos de famille avec les membres éloignés, on peut préférer un dépôt chiffré d'album photo à télécharger plutôt que leur affichage dans un réseau social pour lequel vos correspondants n'ont pas forcément de compte.

Dans le cadre de sa campagne *Dégooglisons Internet*, l'association Framasoft propose une foule de services en ligne. Le but est de démontrer que les logiciels libres sur lesquels sont basés ces services constituent autant d'alternatives sérieuses aux monopoles des services web. Les destinataires sont de deux ordres. D'abord le grand public, qui est ainsi initié à d'autres outils et invité à d'autres usages plus respectueux des données personnelles. Ensuite, les individus (les experts), les associations, les entreprises, qui sont invités à essaimer ces services pour le plus grand nombre.

Tel est l'objectif du mouvement impulsé par Framasoft nommé CHATONS [24], le Collectif des Hébergeurs Associatifs, Transparents, Ouverts, Neutres et Solidaires. Chaque « Chaton » est une association (ou éventuellement un groupement) qui propose des services ouverts et basés sur des logiciels libres, tout en respectant un modèle de charte et un manifeste visant à garantir une éthique respectueuse des intimités numériques.

Ainsi, avant de trouver un « Chaton » autour de chez vous, tester les outils proposés par Framasoft vous permettra de trouver un hébergement en ayant une idée plus précise de vos besoins. Rendez-vous donc sur le site de la campagne Degooglisons-internet.org [25].

Bien sûr, il reste la question du coût. Alors que les grands monopoles proposent des solutions gratuites (avec un ajout de fonctionnalités payantes), il peut sembler difficile de payer pour une

24. `https://chatons.org/`
25. `https://degooglisons-internet.org/`

offre *a priori* similaire. Cependant, les organisations offrant des alternatives libres et éthiques, le font généralement sur des modèles économiques différents :

— organisme à but non lucratif, basé sur le bénévolat, le don et de faibles cotisations visant essentiellement à couvrir les frais d'infrastructures,

— petites sociétés utilisant des solutions de logiciels libres et contribuant au code source des logiciels : elles offrent généralement des tarifs tout à fait abordables pour les particuliers avec des garanties plus que suffisantes.

Par conséquent, en guise de choix, s'il faut éviter les offres gratuites offertes par les géants du web, il faut néanmoins avancer un peu d'argent (quelques euros par an, généralement), tel est le prix de la gratuité du libre : le soutien aux communautés qui les font vivre.

4.4.1 Stocker et synchroniser mes fichiers, mes contacts, mon agenda

Plusieurs logiciels libres permettent de créer un service *cloud* permettant de stocker des données à distance et capable d'effectuer des tâches de synchronisation entre plusieurs machines (votre ordinateur, votre tablette, votre smartphone, etc.).

L'un des plus connus se nomme Nextcloud [26]. Après l'ouverture d'un compte, vous pouvez télécharger un client sur votre machine, qui se chargera de synchroniser un dossier local avec un serveur distant : ce que vous mettez dans ce dossier sera stocké à distance, si vous modifiez le contenu à distance ou sur une autre machine disposant du même accès, votre dossier sera d'autant modifié. Nextcloud dispose d'une interface web, d'un client local, et d'une application smartphone.

26. `https://nextcloud.com/`

Le service Framadrive [27], de Framasoft, propose une instance gratuite pour des comptes limités à 2 Go de données : vous pouvez ainsi tester Nextcloud. Une autre instance, Framagenda [28], propose un service Nextcloud spécialement dédié à la gestion de ses contacts et agendas.

Si vous désirez utiliser un service plus conséquent, vous pouvez ouvrir un compte auprès d'un acteur comme par exemple l'association La Mère Zaclys [29] ou l'entreprise Indiehosters [30]. Ce ne sont que deux exemples : vous pouvez trouver sur Chatons.org [31] une liste d'acteurs prêts à vous accueillir !

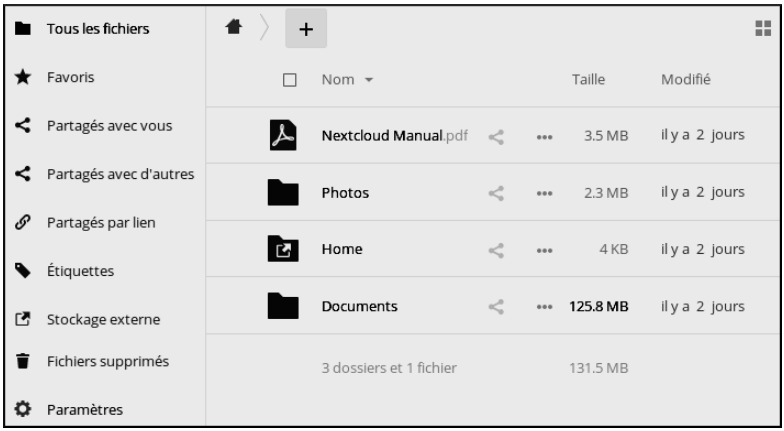


FIGURE 4.6 – Interface web de Nextcloud

4.4.2 Pour correspondre et collaborer

Les services infonuagiques connaissent une grande popularité dans le domaine de la collaboration en ligne. Pour votre association, par exemple, il est intéressant de pouvoir disposer d'un service de sondage pour s'accorder sur la date de la prochaine

27. https://framadrive.org/
28. https://framagenda.org
29. https://www.zaclys.com/
30. https://indiehosters.net/page/home
31. https://chatons.org/

assemblée générale, ou encore d'un tableau blanc où il est possible d'écrire à plusieurs un compte-rendu de manière à gagner du temps et ne pas se confondre dans de multiples échanges de courriel. Vous pouvez aussi avoir besoin d'envoyer à vos correspondants des fichiers encombrants comme vos dernières photos de vacances. De multiples applications dans les nuages sont ainsi disponibles et visent à faciliter le travail en commun et les échanges de données.

Là encore Framasoft, dans le cadre de la campagne Degooglisons-internet.org [32], vous propose une trentaine de services différents, basés sur des solutions de logiciels libres, et même avec un système de chiffrement. Parmi ces services, vous trouverez certainement le logiciel qui répondra à votre besoin et vous pourrez en faire profiter vos correspondants. Citons-en quelques-uns en guise d'illustrations :

— Framadate [33] : pour ouvrir des sondages afin de convenir à plusieurs d'une date de rendez-vous, ou créer un petit sondage classique ;
— Framapic [34] : pour envoyer de manière sécurisée des images ou un album d'images à vos correspondants ;
— Framapad [35] : un traitement de texte où l'on peut collaborer en temps réel à plusieurs pour écrire un document avec, en prime, un module de discussion instantanée ;
— Framatalk [36] : un système sécurisé de conversation vidéo ;
— Framalistes [37] : pour créer et gérer une liste de discussion par courriel ;
— Framaforms [38] : pour réaliser des enquêtes en ligne ;
— Framadrop [39] : pour envoyer de lourds fichiers à vos correspondants ;
— etc.

32. https://degooglisons-internet.org/
33. https://framadate.org/
34. https://framapic.org/
35. https://framapad.org/
36. https://framatalk.org/
37. https://framalistes.org/
38. https://framaforms.org/
39. https://framadrop.org/

Cherchez votre chaton

Le mouvement initié par le collectif Chatons.org[a] a pour objectif d'essaimer ce type de service, sur la base d'une charte de confiance. Vous pouvez ainsi trouver un « Chaton » qui vous fournira ce dont vous avez besoin.

a. `https://chatons.org/`

FIGURE 4.7 – Framadate, un service Framasoft

4.5 L'auto-hébergement

Nous ne saurions terminer cette partie sans mentionner la question de l'auto-hébergement de services. En effet, si vous disposez d'un serveur, qu'il soit chez vous ou loué chez un fournisseur, vous pouvez héberger vos propres solutions basées sur des logiciels libres. Pour vous y aider, chaque service Framasoft dispose d'une rubrique « cultivez votre jardin » qui décrit la manière d'installer les logiciels concernés. Cela suppose néanmoins un certain

niveau d'expertise qu'il vous faut acquérir, bien que cela soit accessible assez facilement. Un autre prérequis est de pouvoir disposer d'un temps suffisant pour maintenir un serveur à jour et assez d'assurance pour en garantir la sécurité.

Des systèmes peuvent néanmoins vous aider à accomplir ces tâches apparemment fastidieuses. En voici deux :

— Yunohost [40] : il permet de déployer plusieurs logiciels à la demande, héberger ainsi ses propres services et éventuellement inviter d'autres utilisateurs à en profiter ;
— Cozycloud [41] : il s'agit d'une solution intégrée de plusieurs logiciels déployés ensemble pour offrir un éventail de services personnels.

Quel que soit votre choix, entre héberger vos propres services ou utiliser ceux d'un tiers, ces solutions démontrent la grande malléabilité des logiciels libres qui permettent de décentraliser les offres et remodeler les chaînes de confiance entre les utilisateurs et les hébergeurs.

40. https://yunohost.org/
41. https://cozy.io/fr/

CHAPITRE 5

Suis-je en sécurité sur Internet ?

En matière de lutte contre les malveillances informatiques, les pratiques des utilisateurs se sont plutôt améliorées ces dernières années. Cela fait suite en particulier aux révélations successives sur la surveillance des firmes et l'affaire du programme de surveillance de la NSA (PRISM[1]) révélé par Edward Snowden. La confiance des utilisateurs envers les plates-formes de service et les logiciels en général a largement baissé, ce qui a causé en retour un effet sur le marché : la recherche individuelle de solutions sécurisées et une modification des stratégies sécuritaires par les entreprises et collectivités. Cela s'est même concrétisé par l'ouverture d'une économie de la confiance avec, comme paradoxe, le fait que les mêmes firmes impliquées dans l'affaire PRISM cherchent à proposer (démontrer) des solutions visant à garantir d'une manière ou d'une autre la confidentialité des utilisateurs. Mais ces derniers ne sont pas dupes.

Évidemment, ces stratégies n'auraient aucune raison d'être poursuivies si, d'un autre côté, les attaques malveillantes ne se

1. https://fr.wikipedia.org/wiki/PRISM_(programme_de_surveillance)

multipliaient pas, menées tant par de puissantes organisations du crime comme par des gagne-petits au pouvoir de nuisance multiplié par les possibilités informatiques. En effet, nombre d'entreprises et collectivités de toutes tailles font régulièrement l'objet de tentatives de fishing [2], attaques par déni de service [3] et de ransomware [4]. Les individus en sont aussi les victimes, très régulièrement, qu'il s'agisse d'arnaques ou de virus. Les pièces jointes dans les courriels sont trop vite ouvertes…

Prism-break

En matière de protection individuelle, le site internet multilingue Prism Break [a] est un bel exemple de mise à disposition de solutions logicielles alternatives pour les utilisateurs qui comprennent de cette manière combien le logiciel libre est important dans ce domaine, à la fois pour se protéger des malveillances mais aussi assurer la confidentialité, la vie privée, face à n'importe quelles intrusions.

a. `https://prism-break.org/fr/`

Qu'entend-on par sécurité ? En fait, il s'agit de trois choses :

1. *la disponibilité des données* : pouvoir accéder à ses données lorsqu'on le souhaite et ne pas toujours dépendre d'un tiers, fût-il de confiance ;
2. *l'intégrité des données* : il faut que les données ne soient pas modifiées sans autorisation ;
3. *la confidentialité* : les données qui m'appartiennent ainsi que les informations que l'on pourrait inférer de mes usages ne doivent pas être accessibles sans autorisation.

Ces trois domaines concernent respectivement :

1. *l'usage de services sur Internet*, en particulier les services liés à la messagerie, au *cloud* et aux réseaux sociaux. À la différence de services centralisés (comme Facebook), la décentralisation

2. `https://fr.wikipedia.org/wiki/Hame%C3%A7onnage`
3. `https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service`
4. `https://fr.wikipedia.org/wiki/Ransomware`

de ce type de services (comme le réseau Diaspora*) permet de réduire les risques de rupture (ou de censure). Il faut donc bien choisir les services que l'on utilise en connaissance de cause. Pour ce qui concerne l'usage informatique en local, la bonne santé de votre machine, les mises à jour des logiciels, et tout un ensemble de pratiques rigoureuses vous permettront d'assurer la disponibilité de vos données ;

2. *la neutralité des réseaux* : le transfert de données ne doit pas modifier les données. Que diriez-vous si votre facteur ouvrait votre courrier, faisait une copie de la lettre pour réduire sa taille (au risque de perdre de la lisibilité ou même en coupant des parties), prenait une enveloppe plus petite et vous donnait le résultat ? C'est pourtant ce que certains fournisseurs d'accès souhaiteraient faire au nom de l'économie de bande passante. Bien sûr, l'intégrité de vos données est plus directement menacée par les actes de malveillance (piratage). Pour s'en prémunir, il faut là encore employer des logiciels sûrs, lutter contre les vulnérabilités aux virus, ne pas utiliser des services qui modifient les contenus ou se les approprient ;
3. *les risques liés à la surveillance*, qu'il s'agisse de votre voisin, de firmes ou d'États. Ce genre de pratique ne met pas seulement en jeu les intimités numériques, car si nous nous sentons surveillés, nous censurons automatiquement nos propos. Dès lors, on comprend pourquoi la liberté d'expression est l'une des premières libertés menacées par la surveillance sur Internet.

Toutes ces questions peuvent être regroupées en une seule : *quelle confiance puis-je accorder aux dispositifs numériques, aux logiciels et aux services que j'utilise ?* Cette confiance ne peut pas être aveugle. Par exemple, même si vous avez *a priori* confiance envers votre fournisseur d'accès, il est probable que vous seriez plus serein si les courriels que vous envoyez à votre banquier étaient chiffrés de manière à ce que seul votre banquier puisse les lire.

La confiance nécessite donc à la fois une expertise et des pratiques. Or tout le monde n'a pas l'expertise suffisante pour évaluer la confiance envers les logiciels et les services. C'est pour cela que

l'utilisation d'outils libres, dont le code source est ouvert, permet de faire reposer cette expertise sur un collectif nombreux de pairs plutôt que sur une personne, entreprise ou institution. Il en va de même pour les services en ligne, qui peuvent reposer sur des solutions de logiciels libres. Quant aux pratiques, ce sont d'elles que nous allons parler dans ce chapitre : la sécurisation des dispositifs, le chiffrement, la protection des accès.

Rejoignez la SecNumacadémie

En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a lancé un MOOC (*massive open online course*) ouvert à tous dans le but de sensibiliser à la sécurité informatique. Très pédagogique et progressif, ce MOOC est largement conseillé pour prendre la mesure des enjeux de la sécurité et des bonnes pratiques, au quotidien comme dans la vie professionnelle. Une adresse : `secnumacademie.gouv.fr`.

5.1 Protéger mes dispositifs

Qu'il s'agisse de votre ordinateur ou de votre smartphone, vous ne souhaitez pas que n'importe qui puisse accéder à vos données. Si les systèmes d'exploitation insistent bien souvent sur la création d'un mot de passe garantissant l'ouverture des sessions, trop nombreux sont les utilisateurs qui passent outre cette recommandation. Ce n'est cependant qu'une faille parmi d'autres contre les malveillances dont vous pouvez faire l'objet.

5.1.1 Sessions et profils d'utilisateurs

Oui, il est pénible de devoir entrer un mot de passe à chaque fois que l'on souhaite accéder à sa machine après un temps d'inactivité. Mais il faut avouer que le prix est peu cher payé pour un premier niveau élémentaire de protection. Qui a perdu son téléphone

portable sans sécurisation de la session… n'a plus qu'à trouver très vite un autre moyen de se rendre sur les différents services utilisés pour en changer les accès, tout en espérant que le voleur n'ira pas trop fouiller dans les photos et autres documents stockés dans la mémoire.

Toutefois, si vous avez perdu votre ordinateur, tablette, ou smartphone, avec ou sans mot de passe, vous avez de toute façon un grand intérêt à changer vos autres accès : quel que soit le système d'exploitation, les mots de passe de session, voire les mots de passe d'administration, sont en général assez rapides à contourner ou à cracker.

Profils et sessions

Prenez le temps de réfléchir à l'usage que vous comptez faire de votre machine. Si d'autres utilisateurs en auront l'accès, utilisez des profils, c'est-à-dire des comptes personnels qui permettront d'une part à tous les utilisateurs d'organiser leurs sessions comme ils l'entendent, et d'autre part leur éviteront d'accéder aux données des uns et des autres.

Même si vous êtes seul-e à utiliser votre machine, créez au moins deux comptes : un compte disposant des droits d'administration et un autre dédié à l'utilisation (un profil utilisateur[5]). Il sera ainsi plus difficile pour un programme malveillant d'installer des fichiers visant à modifier le système. Cette recommandation vaut en particulier pour les possesseurs de Windows. En effet, sous GNU/Linux cette précaution élémentaire est déjà comprise dans le quotidien : un profil d'administration est toujours nécessaire pour installer un logiciel ou modifier un « fichier système ». Notez aussi que le navigateur Firefox dispose d'une fonction dédiée à la gestion de profils.

5. https://fr.wikipedia.org/wiki/Profil_utilisateur

5.1.2 Virus et antivirus

Un logiciel antivirus est conçu pour identifier et neutraliser des programmes dont le comportement est suspect. En réalité, les virus informatiques ne sont qu'une catégorie de *logiciels malveillants* [6]. Cette catégorie regroupe :

— *les virus* : ils se répliquent et se propagent à l'aide de fichiers « hôtes » (par exemple, un document texte que l'on ouvre par habitude). Ils peuvent infecter l'amorçage de la machine, les fichiers, le fonctionnement des programmes déjà existants… Un comportement classique d'un virus bien fait consiste à s'installer et effectuer des tâches de manière dissimulée (son fonctionnement passe inaperçu aux yeux de l'utilisateur). Un virus peut ainsi chiffrer un disque dur, envoyer son contenu quelque part et demander une rançon.

— *les vers* : ils se propagent d'eux-mêmes de machine en machine, notamment à travers le réseau (courrier électronique, partage de fichier, etc.)

— *les chevaux de Troie* : ils utilisent des portes dérobées (ou en ouvrent selon les besoins). Par exemple le développeur d'un logiciel peut laisser une entrée discrète (*backdoor*) au programme pour surveiller l'usage du logiciel ou même en prendre le contrôle. Nombre d'entreprises pratiquent ce genre de chose, à commencer par les plus connues comme Microsoft [7].

5.1.2.1 Fonctionnement

Les logiciels antivirus agissent donc à de multiples niveaux sur la machine. Ils disposent habituellement de deux « grandes fonctionnalités » : les tâches de *firewall* [8] qui consistent à surveiller

6. `https://fr.wikipedia.org/wiki/Logiciel_malveillant`

7. Par exemple, pour optimiser sa stratégie de propagation de Windows 10, Microsoft a en effet utilisé des portes dérobées sous Windows 7 et 8 en modifiant un avertissement indiquant que la mise à jour vers Windows 10 devait être faite, même si l'utilisateur l'avait préalablement refusée. Pour cela une porte dérobée a été utilisée à l'insu des utilisateurs. Voir Gregg Keizer, « Microsoft sets stage for massive Windows 10 upgrade strategy », *ComputerWorld*, 07/12/2015.

8. Littéralement un *pare-feu* : il consiste à mettre en place une politique de sécurité réseau. Il est toutefois préférable d'utiliser un *firewall* plus complet que les

les activités réseaux de la machine et les tâches d'anti-virus proprement dites, c'est à dire la surveillance des exécutions des programmes et des emplois de fichiers. Mais il leur faut généralement une base de donnée dans laquelle ils puisent des éléments de comparaison pour identifier les virus. C'est la raison pour laquelle un logiciel antivirus doit impérativement être mis à jour, c'est-à-dire lui permettre de télécharger, depuis le site du fournisseur, les *dictionnaires* qui permettent d'avoir toutes les informations utiles.

Une seconde stratégie utilisée par les logiciels antivirus, consiste non plus à identifier des logiciels malveillants mais à assister l'administrateur de la machine pour éviter les infections. Pour cela, il peut bloquer par défaut toute exécution de programme à l'exception de ceux pour lesquels l'administrateur a donné son accord.

Une troisième stratégie consiste en une méthode d'apprentissage. Les virus, à moins d'être extrêmement bien dissimulés, ont par définition un comportement suspect. Par exemple ils peuvent solliciter un programme en cours d'exécution ou tenter de supprimer / modifier des fichiers de manière inhabituelle. Le logiciel antivirus émet alors une alerte à l'intention de l'utilisateur.

Vous noterez que les deux dernières stratégies supposent une expertise de la part de l'utilisateur. Bien souvent, c'est la principale faille du système : submergé par les alertes, ou ne sachant exactement quelle attitude employer (souvent parce que le manuel de l'antivirus n'est pas lu ou trop complexe), l'utilisateur clique un peu au hasard.

5.1.2.2 Que choisir ?

Dans l'ensemble, un logiciel antivirus performant est nécessaire : c'est toujours à l'utilisateur qu'il revient de choisir. Voici quelques éléments de comparaison :

— l'efficacité : le logiciel dispose-t-il d'une base de données reconnue comme étant importante et fiable ? Qui est son créateur et est-il reconnu ? Il faut se renseigner ;

seules fonctions offertes par les logiciels anti-virus, même si elles couvrent les besoins immédiats.

— l'impact de l'antivirus sur les performances de la machine : souvent gourmands en ressources mémoire, car ils fonctionnent en permanence, les antivirus ne sont pas tous logés à la même enseigne ;
— la complexité du fonctionnement et le paramétrage : les néophytes ne devraient pas utiliser des antivirus trop complexes, au risque de bénéficier d'une efficacité dégradée ;
— l'interface : est-il facile d'utiliser le programme ? les alertes sont-elles claires et assez compréhensibles pour ne pas perdre trop de temps ?

Le choix d'un logiciel antivirus dépend donc de plusieurs paramètres. Mais nous en avons volontairement omis : le fait que le logiciel soit libre ou non. S'il n'est pas libre, vous devez faire confiance au fournisseur, sans toutefois oublier que, si le logiciel est payant et non-libre, son prix n'est pas forcément un gage d'efficacité, et si le logiciel est gratuit et non-libre, il faut se demander comment il est maintenu et par quels moyens.

Comme nous le répétons souvent : l'un des avantages des logiciels libres, c'est que le développement est communautaire. Un logiciel libre qui dispose d'une grande communauté, est un logiciel réputé efficace. C'est le cas de Clamav [9], un logiciel qui dispose, grâce aux remontées de la communauté des utilisateurs, d'une des plus grandes bases de données de signatures virales, c'est-à-dire autant de moyens d'identifier un virus.

Clamav est d'abord un logiciel créé pour les systèmes de type Unix (GNU/Linux ou MacOS). En effet, les serveurs de courriels sont majoritairement installés sur de tels systèmes, il est dès lors important de protéger les utilisateurs, en particulier ceux sous Windows. Or, comme la base de données de Clamav est libre, d'autres anti-virus libres, destinés en particulier à Windows, peuvent en profiter :

— MoonSecure Antivirus [10] : il offre une protection en temps réel avec une interface simple (bien qu'un peu vieillotte),

9. `http://www.clamav.net/`
10. `http://moonsecure.net/df/`

tout en profitant de la base de Clamav. On peut bien sûr scanner des fichiers et des disques à la demande ;
— Clamwin [11] assure l'analyse des fichiers et disques en profitant lui aussi de la base de Clamav par contre il n'offre pas de protection en temps réel. Cette dernière tâche est assurée par son binôme, Clam Sentinel [12].

Les anti-virus ne peuvent pas tout

L'usage seul de ces logiciels (libres ou non) n'est en aucun cas une garantie contre les logiciels malveillants. Dans tous les cas, le meilleur moyen de s'en prémunir consiste à adopter des pratiques : ne pas télécharger ni installer de logiciels depuis d'autres sites que les sites officiels, se méfier des applications gratuites et non-libres (et même si elles sont libres, renseignez-vous sur la communauté), ne vous rendez pas sur des sites douteux, n'ouvrez pas les pièces jointes à vos messages sans d'abord en identifier la nature et la provenance, etc.

5.1.3 Logiciels malveillants et systèmes d'exploitation

Pour le résumer en quelques mots, un virus informatique exploite des failles de sécurité. Dans ce domaine, aucun système d'exploitation n'est invulnérable. Cependant, tous les systèmes d'exploitation ne sont pas logés à la même enseigne.

Protéger un ordinateur sous Windows suppose une attention de tous les instants et requiert, en plus de bonnes pratiques d'usage, une méfiance quasi-systématique, y compris vis-à-vis du système lui-même qui dépend des stratégies de la firme Microsoft. On peut en dire autant de la part de MacOS et d'autres systèmes. Sur une page intitulée « Le logiciel privateur est souvent malveillant [13] », le

11. http://www.clamwin.com/
12. http://clamsentinel.sourceforge.net/
13. https://www.gnu.org/proprietary/proprietary.html

site de la Free Software Foundation recense des exemples de malveillance de la part des logiciels privateurs ; on peut y faire une recherche selon le type de malveillance et le nom des firmes.

Ces griefs adressés aux systèmes d'exploitation propriétaires ne signifient pas pour autant que les systèmes libres comme GNU/-Linux sont exempts de toute vulnérabilité. La différence, c'est que profitant d'une transparence dans le développement communautaire, lorsqu'une faille est découverte, il faut très peu de temps pour la corriger et propager la correction. Par exemple la vulnérabilité Heartbleed, qui concernait les clés de chiffrement sous Linux (risque de les voir récupérées par des personnes mal intentionnées), a été découverte en mars 2014, rendue publique le 7 avril et les correctifs étaient déjà disponibles.

On peut s'amuser à comparer Windows et GNU/Linux pour comprendre pourquoi le second est mieux protégé par défaut contre les malveillances. Sur le tableau 5.1 on voit que les risques sont finalement assez similaires, qu'on utilise Windows ou GNU/-Linux : tout est une question de pratique, de savoir activer des fonctionnalités ou ne pas le faire, etc. Pour autant, à moins d'être obligé-e d'utiliser Windows, il vaut mieux employer une distribution GNU/Linux non pas pour être sûr d'être protégé-e contre les malveillances, mais pour avoir à disposition un système plus difficilement attaquable.

Une autre opportunité, non pour se prémunir des logiciels malveillants mais pour protéger ses données, consiste à les *chiffrer*. Aujourd'hui les systèmes d'exploitation proposent la possibilité de chiffrement dès l'installation : Windows avec Bitlocker, MacOS avec Filevault, les distributions GNU/Linux avec l'outil de partitionnement LVM qui propose une option de chiffrement, etc. Les outils ne manquent pas. Et à condition de bien comprendre ce que l'on fait et de ne pas perdre ses clés, chiffrer ses données est encore le meilleur moyen de se protéger à la fois contre les malveillances et contre les surveillances. Encore faut-il ne pas se contenter de chiffrer les données sur son disque, mais de considérer tout transfert d'information comme une faille potentielle.

Windows	GNU/Linux
Il faut créer volontairement au moins un compte utilisateur pour éviter que toutes les sessions ne se fassent avec des droits d'administration.	Les droits d'administrateur et les droits d'utilisateur sont d'emblée différenciés : un utilisateur n'a pas les droits de modification des fichiers système.
Les installations domestiques de Windows sont similaires, elles différencient seulement en fonction de la version de Windows (votre Windows 7 ressemblera au Windows 7 de votre voisin).	Il existe une multitude de distributions GNU/Linux différentes, avec des arrangements très différents (deux installations de la même distribution peuvent être configurées à tel point qu'elles ne se ressemblent plus).
Les fichiers exécutables peuvent être installés facilement (leur blocage n'est pas activé par défaut).	Il faut déclarer les droits d'exécution d'un fichier avant de l'utiliser comme exécutable.
Les failles mettent parfois plusieurs mois à être corrigées.	Grande réactivité de la communauté, failles corrigées rapidement.
Le système est une boîte noire et n'est auditable que par les ayants-droits.	Le code source est ouvert, un maximum d'acteurs, y compris de haut niveau, peuvent identifier les failles.
Il existe un *store* (magasin) d'application mais l'installation de programmes est souvent anarchique : trop de téléchargements et d'installations se font en récupérant des fichiers exécutables sur des sites peu sûrs.	La plupart des utilisateurs utilisent les dépôts officiels de leur distribution GNU/Linux pour installer des programmes, mais les utilisateurs utilisent parfois des dépôts non-officiels sans en évaluer le risque.

TABLEAU 5.1 – Comparatif (non exhaustif et un peu partial) entre les deux OS

5.2 Chiffrer mes données

Le chiffrement des communications est d'abord un outil. Lorsque vous communiquez avec votre banque ou que vous effectuez un paiement en ligne, vous devez vous assurer que vos communications sont bel et bien chiffrées de manière à ne pas courir le risque de les voir interceptées et copiées. N'oubliez pas : ce que vous faites en ligne, les messages que vous envoyez comme les

sites que vous visitez, tout cela est une affaire de copie de contenus sur des serveurs et sur votre ordinateur (voir la section Navigation). Par exemple, même si *a priori* vous pouvez faire confiance aux employés de votre fournisseur d'accès, vous ne pouvez pas leur faire suffisamment confiance pour leur confier dans un courriel écrit en clair votre numéro de carte bancaire ou des informations relatives à votre état de santé.

Ajoutons à cela que, depuis l'affaire Snowden, nous savons que des firmes et des États mettent en œuvre des pratiques de surveillance des communications des citoyens : que ces pratiques évoluent, qu'un gouvernement soit ou non assez totalitaire pour retenir contre vous des informations *a priori* anodines, que vous le souhaitiez ou non, il est important que les citoyens puissent avoir à leur disposition un moyen d'échanger des informations de manière secrète… cela s'appelle de l'intimité numérique, exactement comme lorsque vous fermez la porte de votre salle de bain. Pour avoir accès à un moyen de garder au secret certaines de vos données et de vos correspondances dans le monde numérique, et donc exercer pleinement votre droit à la vie privée, vous devez savoir comment chiffrer des informations. C'est l'objet des prochaines sections.

5.2.1 Pretty Good Privacy

Avant de commencer les explications, allons droit au but. De cette manière, si les prochains paragraphes vous semblent laborieux, l'essentiel vous sera familier.

Imaginez une boîte, avec une serrure, qui enferme vos informations. Chacun de vos correspondants peut placer quelque chose dans cette boîte grâce à une formule et vous seul avez la clé qui permet de l'ouvrir. Tel est, de manière simplifiée et imagée, la méthode de chiffrement que nous allons expliquer, sauf que nous n'allons parler que de clés. Accrochez-vous ça commence.

L'un des premiers outils de chiffrement accessible à tous se nomme Pretty Good Privacy (PGP). Ce programme fut créé par Philip Zimmermann. Son histoire débute dans les années 1980 et le combat qui fut mené consista essentiellement à rendre PGP légal.

On comprend aisément qu'un gouvernement considère de manière plutôt négative le fait que des citoyens puissent avoir accès à un système qui, par des lois mathématiques, rend impossible la lecture des messages qu'ils s'envoient.

PGP appartient à la PGP Corporation [14] or, en 1998, cette société a rompu avec le principe de livrer le code source pour assurer une révision par les pairs. En 2002, le code source est de nouveau disponible, mais entre temps, PGP a donné lieu à un standard proposé par l'IETF (Internet Engineering Task Force) nommé Open-PGP et décrit dans la RFC 2440 [15]. Suivant ce standard, le système GnuPG (Gnu Privacy Guard) fut créé, entièrement libre et par ailleurs agréé par Philip Zimmermann.

PGP est un système de chiffrement à clé publique [16]. Pour comprendre de quoi il s'agit, il faut comparer ce système à un système de chiffrement symétrique. Tout le monde connaît le chiffrement symétrique : il s'agit d'utiliser la même clé pour chiffrer et déchiffrer un message. Fred envoie un message à Katy et le chiffre avec une table de correspondance entre les lettres de l'alphabet et des symboles. Katy et Fred doivent avoir la même clé (la table de correspondance) pour pouvoir chiffrer et déchiffrer leurs messages. Tout le problème est de faire circuler cette table / clé de manière secrète entre Katy et Fred.

Le chiffrement à clé publique (ou asymétrique) présente un avantage majeur sur le chiffrement symétrique : *seules circulent les clés publiques et le déchiffrement appartient au destinataire seulement*. En effet, au départ, les correspondants se créent chacun un couple de clé publique et clé privée. Si les clés publiques peuvent être connues et utilisées par n'importe qui, les messages chiffrés avec une clé publique ne peuvent être déchiffrés qu'avec la clé privée qui lui correspond. Le problème de la circulation des clés de chiffrement est résolu.

14. `http://www.pgp.com`
15. `https://www.ietf.org/rfc/rfc2440.txt`
16. Pas vraiment, il est en fait hybride : comme on le verra plus loin, PGP utilise un couple clé privée / clé publique mais ajoute à cela l'empaquetage des messages avec leur clé de déchiffrement et ce sont ces clés que les clés publiques et privées permettent de récupérer pour déchiffrer les messages.

Le cas de PGP est particulier dans ce domaine, puisqu'il ne se contente pas de chiffrer avec une clé publique. Une autre clé entre en jeu : la clé de session. Lorsque je chiffre un texte avec PGP, je le chiffre avec une clé de session générée sur le moment et de manière aléatoire. Ensuite, cette clé de session et le message chiffré sont compressés ensemble et chiffrés avec la clé publique du destinataire. Le destinataire, quant à lui, récupère la clé de session grâce à sa clé privée et peut alors déchiffrer mon message.

Pourquoi, en quelque sorte, ce chiffrement en deux temps ? En fait, ce que le destinataire déchiffre en premier, c'est l'en-tête du message, de manière à l'authentifier. Ensuite seulement il déchiffre le message grâce à la clé de session récupérée. Cela rend PGP très sûr : chaque message possède sa propre clé et chaque clé de message doit correspondre à la clé privée du destinataire. Si je veux casser PGP, il faut que je casse à chaque fois le couple clé privée / clé de session.

Par ailleurs, une autre fonction de PGP est l'authentification de l'expéditeur (la signature). Pour chaque message envoyé, PGP applique une fonction de hachage avec la clé privée de l'expéditeur : c'est le calcul d'une empreinte unique (un sceau) qui est jointe au texte et qui fait que, lorsque je reçois le message, je peux comparer cette empreinte avec celle que je calcule, cette fois, avec la clé publique de l'expéditeur. Je suis alors certain qu'il vient de mon correspondant.

Ajoutons à cela l'avantage de la compression. Un texte, aussi chiffré soit-il, peut toujours présenter des régularités. On peut par exemple en tirer des statistiques sur l'emploi de tels caractères et en inférer du sens. Souvenez-vous des magazines de votre enfance où vous deviez déchiffrer un message en trouvant les lettres des mots selon leurs fréquences et leurs probabilités. La compression d'un message permet de briser cette « logique » et ajoute un surplus de sécurité.

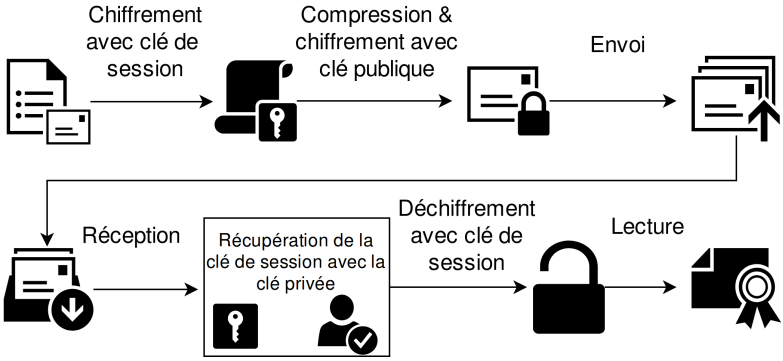
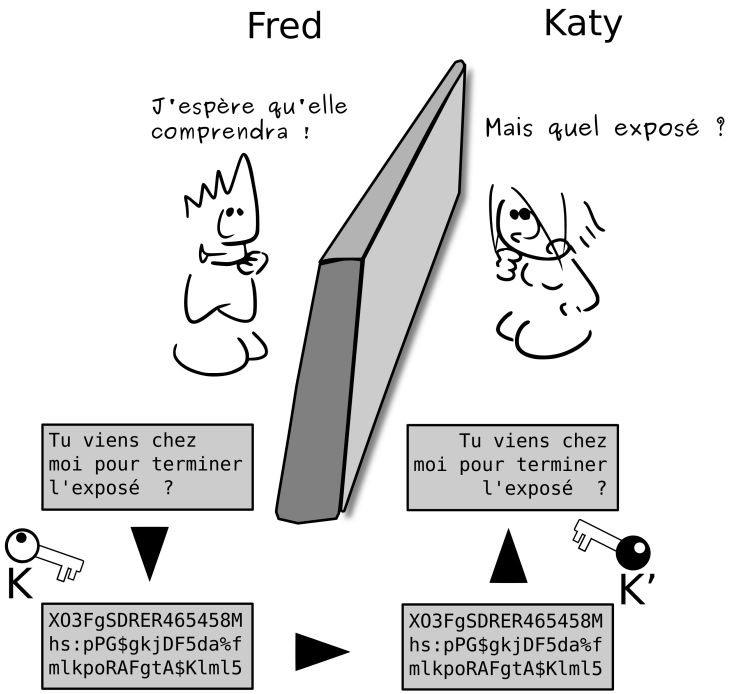


FIGURE 5.1 – Fonctionnement de PGP

Dans les faits, si l'explication de PGP n'est pas évidente, son utilisation est assez simple. On peut se contenter de cette affirmation : chaque correspondant possède une clé privée et une clé publique ; les clés publiques sont diffusées et tous les messages chiffrés à l'aide de la clé publique d'un correspondant ne pourront être déchiffrés qu'avec la clé privée de ce correspondant. Dans l'illustration, Fred envoie un message chiffré à l'aide de la clé publique (K) de Katy. Cette dernière peut alors déchiffrer le message avec sa clé privée (K'). Pour lui répondre, Katy utilisera la clé publique de Fred et ce dernier pourra déchiffrer à l'aide de sa clé privée à lui. Ce que fait PGP en sous-main (hachage, empreinte et clé de session) peut parfaitement être invisible pour l'utilisateur.

5.2.2 À quoi bon ?

Chiffrer un contenu, cela revient à utiliser une clé de chiffrement pour faire deux choses : rendre impossible la compréhension d'une information et l'authentifier. En effet, une clé de chiffrement peut être utilisée à la fois pour chiffrer tout un message et pour le signer. Une telle clé est donc à la fois un outil servant le secret des communications mais aussi une solution permettant d'instaurer un système de confiance entre l'émetteur et le récepteur.


Fred
Katy
J'espère qu'elle comprendra !
Mais quel exposé ?
Tu viens chez moi pour terminer l'exposé ?
Tu viens chez moi pour terminer l'exposé ?
K
K'
XO3FgSDRER465458M hs:pPG$gkjDF5da%f mlkpoRAFgtA$Klml5
XO3FgSDRER465458M hs:pPG$gkjDF5da%f mlkpoRAFgtA$Klml5

Générer soi-même ses clés et envoyer les clés publiques à des correspondants suppose de maîtriser les flux d'informations. Recevoir un message chiffré ne signifie pas pour autant que l'on puisse faire confiance à l'émetteur. Si je reçois un message chiffré de la part d'un correspondant inconnu qui utilise ma clé publique pour le faire, je n'ai pas d'autre moyen que de faire connaissance avec ce nouveau correspondant pour m'assurer de son identité et faire confiance à l'avenir aux futurs messages qu'il m'enverra. De même, le contenu d'un message chiffré n'est pas forcément doté de bonnes intentions. Il faut donc bien séparer plusieurs notions : le chiffrement, la sécurité et l'authentification.

Une solution consiste à faire reposer la confiance sur une autorité de certification [17]. Il s'agit la plupart du temps de sociétés dûment contrôlées qui endossent le niveau de confiance en proposant des certificats. Par exemple, l'ANSSI tient à jour sur son site [18] la liste des prestataires de confiance contrôlés par l'État Français. De tels prestataires proposent leurs services afin de permettre d'établir des connexions de confiance sur Internet (nous le verrons plus loin dans ce chapitre à propos de HTTPS) c'est-à-dire qu'ils *certifient* des clés de chiffrement. S'il est certifié par une autorité, l'interlocuteur qui m'envoie un contenu chiffré grâce à ma clé publique est *a priori* digne de confiance. Non seulement ce qu'il m'envoie est confidentiel mais, en plus, la forme engage la responsabilité d'un tiers de confiance.

Bien sûr, tous les utilisateurs n'ont pas à acheter de tels services pour leurs besoins quotidiens. Il est possible d'instaurer une chaîne de confiance à partir du moment où les clés sont partagées de manière à ce que chaque correspondant sache à quoi s'en tenir. Un message circulant en clair sur le réseau sera toujours susceptible d'être lu par un tiers. S'il est chiffré, il peut toujours y avoir une usurpation dans la manipulation des clés. Qu'il y ai ou non l'intervention d'une certification, tous les contenus qui circulent sur un réseau sont par nature sujets au risque de piratage.

17. https://fr.wikipedia.org/wiki/Autorité_de_certification
18. https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance

Loin d'annuler complètement ces risques, un chiffrement a l'avantage de renforcer significativement le niveau de confidentialité d'un message. Même si je signe moi-même ma clé de chiffrement, sans certification attestée par une autorité, et que je confie ma clé publique à mes correspondants, les messages chiffrés que je recevrai ou que j'enverrai auront au moins l'avantage de pas être compréhensibles par quelqu'un d'autre. En théorie, si tout le monde appliquait le chiffrement des contenus échangés sur Internet, le niveau de sécurité global serait largement multiplié, même si tout le monde n'utilise pas les services d'autorités de certification. Évidemment, chiffrer ses propres fichiers et dossiers, voire son disque dur tout entier, est une précaution qui permettrait de lutter efficacement contre tous les virus de type *ransomware* (qui chiffrent les données pour lesquelles les pirates réclament de l'argent en échange de la clé). Ceci sans compter la possibilité de conserver en sécurité des données sensibles ou tout simplement personnelles (les copies de vos papiers d'identité, vos feuilles d'impôt, vos ordonnances médicales, etc.)

En d'autres termes, le chiffrement à l'aide de logiciels libres (en particulier GnuPG – GNU Privacy Guard, l'implémentation du standard OpenPGP) permet de mettre à disposition de tous un moyen d'exercer efficacement le secret des correspondances. Il importe de prendre conscience que cette possibilité est fragile et parfois menacée, alors qu'elle relève clairement de l'exercice du droit à la vie privée si cher aux pays démocratiques.

Pour utiliser des solutions de chiffrement, on peut faire confiance à un service de messagerie incluant d'emblée un système de chiffrement, on peut aussi gérer soi-même ses clés de chiffrement et utiliser des logiciels spécifiques. Tout repose sur deux approches complémentaires des outils : évaluer le degré de confiance et intégrer le chiffrement dans des pratiques quotidiennes.

5.2.3 Faire confiance

Nous avons vu dans le chapitre 3 que pour envoyer des courriels, beaucoup de services proposent des messageries en ligne,

FIGURE 5.2 – Utiliser ses clés avec discernement

comme des *webmail*. Certains prestataires offrent de surcroît la possibilité de chiffrer les messages à l'aide d'un système de chiffrement asymétrique comme PGP.

Or, nous avons vu aussi que pour chiffrer de cette manière, il faut générer deux clés, l'une privée (à mettre en lieu sûr) et l'autre publique (à distribuer). Dès lors, si de tels services proposent le chiffrement des contenus en un clic pour leurs utilisateurs, ils présentent l'avantage de largement simplifier l'usage du chiffrement, mais en retour il leur faut gagner la confiance des utilisateurs qui leur confient la gestion à la fois de la clé privée et de la clé publique. De ce point de vue, tous les services ne sont pas égaux, et certains sont bien moins sérieux que d'autres. Il est important d'en évaluer la portée.

Nous pouvons citer Protonmail [19], un service de *webmail* gratuit (pour les fonctionnalités de base) construit sur des logiciels libres. Il propose un chiffrement dit « de bout en bout », c'est-à-dire que

19. `https://protonmail.com`

seuls les correspondants peuvent chiffrer et déchiffrer leurs messages, et l'hébergeur n'a aucun moyen de les lire. Conscientes du problème lié à la gestion des clés dont Protonmail endosse la responsabilité et la confidentialité, les équipes de Protonmail ont mis au point un système qui permet de chiffrer les clés privées sur les serveurs de manière à ce que seul l'utilisateur-propriétaire de la clé puisse l'utiliser. L'ensemble du dispositif de Protonmail fait l'objet d'audits réguliers, dans une transparence relative que peu de services du genre sont en mesure de fournir. Dès lors, si le choix revient toujours à savoir où placer le curseur de confiance, et si tous les utilisateurs sont loin d'être capables d'auditer un tel service, les efforts de transparence et la lecture des avis éclairés peuvent constituer de bons indices.

Un tiers peut donc gérer complètement les clés nécessaires à un chiffrement efficace. Le prix à payer en retour de cette facilité d'usage, c'est la confiance. Mais d'autres systèmes de communication permettent de concentrer chez l'utilisateur les outils du chiffrement tout en permettant d'automatiser l'usage à un point tel qu'il passe presque inaperçu.

C'est le cas de l'application Signal [20], une application mobile (il existe une version autonome pour ordinateur) qui permet les communications écrites, audio et vidéo. Signal utilise un protocole particulier et libre, justement nommé *Signal Protocol*, qui permet un chiffrement de bout en bout. Ce protocole est utilisé par d'autres applications connues, et son histoire atteste largement de son efficacité. Du point de vue de l'utilisation, le chiffrement s'effectue de manière totalement automatisée entre les correspondants. Du point de vue de l'utilisateur, au lieu d'avoir à évaluer la confiance au regard du niveau de transparence d'un hébergeur, il doit placer sa confiance dans la structure du logiciel et la communauté des développeurs de ce logiciel libre.

Avec ces deux exemples, on peut conclure que la confiance en un logiciel de communication chiffrée ne s'attribue pas à la légère. Pour certains utilisateurs dans des contextes politiques ou sociaux dangereux, il peut même s'agir d'une question de vie ou de mort.

20. `https://signal.org/`

Même si l'utilisateur n'est ni développeur ni spécialiste de la sécurité informatique, au moins trois questions complémentaires se posent :

1. le dispositif repose-t-il sur un ou plusieurs logiciels ou protocoles libres ? dans ce cas, les évaluations et les qualifications sont publiquement disponibles ;
2. le développement ou le service hébergé sont-ils transparents vis-à-vis des utilisateurs ? dans ce cas, il s'agit de savoir si l'on peut adhérer aux principes et aux intentions des prestataires ou de la communauté de développement ;
3. existe-t-il suffisamment de documentation, assez vulgarisée et claire sur les fonctionnalités des dispositifs et leurs évaluations ? dans ce cas, c'est un gage d'honnêteté.

La surveillance est une industrie

Un récent rapport de Cracked Lab[a], intitulé *Corporate surveillance in Everyday Life* (2017) a examiné les pratiques de l'industrie de l'exploitation des *big datas*. Il en ressort que si le pistage et le profilage des individus est une activité extrêmement lucrative, elle profite aussi de développements technologiques spectaculaires et devient un instrument de contrôle social. Chiffrer ses données, c'est tâcher de laisser le moins de traces possible de son quotidien mais c'est aussi protéger la vie privée de tous.

a. https://framablog.org/2017/10/25/comment-les-entreprises-surveillent-notre-quotidien

Quels que soient ses choix en matière de communication, il est nécessaire de savoir chiffrer par soi-même des informations, à commencer par des contenus qui n'ont pas forcément vocation à être échangés. En effet, un service aussi efficace soit-il peut toujours fermer ses portes de manière plus ou moins contrainte (ce fut le cas du service de courriel Lavabit[21] en 2013), et un logiciel « clés

21. https://fr.wikipedia.org/wiki/Lavabit

en mains » peut toujours manquer de développement et devenir obsolète, ce qui est vrai aussi pour les protocoles. Là encore, c'est vers des dispositifs comme GnuPG (OpenPGP) que nous devons nous tourner. Nous allons voir que dans l'usage quotidien du chiffrement asymétrique, il n'y a rien de bien complexe, et que grâce à quelques assistants bien faits, chiffrer est réellement à la portée de tous.

5.2.4 Le chiffrement par l'exemple

Concrètement, lorsque je chiffre un contenu, qu'est-ce que je demande à la machine ? Après avoir installé GnuPG qui me permet d'utiliser un standard de chiffrement PGP, je lui demande :

1. de faire un calcul sur les informations à chiffrer et utiliser une clé publique pour cela (la mienne ou celle d'un destinataire),
2. de produire un résultat (des données) illisible sans la clé,
3. de signer ce résultat, toujours à l'aide de ma clé, c'est-à-dire créer une empreinte à chiffrer pour produire une signature dont l'authentification sera possible avec ma clé ou celle d'un destinataire (cette signature permet aussi de vérifier l'intégrité du contenu chiffré et savoir s'il a été modifié).

Pour accomplir ces opérations, votre machine a besoin d'un programme qui lui permet d'effectuer les calculs et d'utiliser un protocole de chiffrement. Pour utiliser OpenPGP, la première étape consiste à se procurer le logiciel GnuPG [22]. Il est disponible pour la plupart des systèmes d'exploitation, y compris pour des appareils mobiles, depuis le site officiel gnupg.org [23]. Téléchargez et installez.

Dans un second temps, vous pouvez vous pencher sur le manuel de GnuPG [24]. Mais sans toutefois vous formaliser : rassurez-vous, un usage classique n'est pas aussi complexe qu'au premier abord.

22. Vous pouvez aussi lire avec intérêt cet article de David Legrand, « OpenPGP et GnuPG : 25 ans de chiffrement pour tous, ce qu'il faut savoir avant de s'y mettre », *NextInpact*, 27/12/2016.
23. `https://www.gnupg.org/`
24. `https://www.gnupg.org/gph/fr/manual.html`

5.2.4.1 Ne pas perdre ses clés et savoir s'en servir

De la génération de clés au chiffrement de contenus, tout cela est faisable à la ligne de commande sous n'importe quel système d'exploitation. Cependant, à moins d'être très à l'aise avec le Terminal, où pour un apprentissage pédagogique, utiliser la ligne de commande n'est pas toujours ce qu'il y a de plus attirant. C'est pourquoi des interfaces graphiques ont été créés, qui permettent d'utiliser GnuPG, de gérer des clés (les vôtres et celles des destinataires) et d'effectuer des opérations de chiffrement de manière assez intuitive.

On peut prendre l'exemple de GPA (GNU Privacy Assistant [25]). Complémentaire à GnuPG, GPA est un assistant de gestion de clés de chiffrement simple à l'utilisation et qui permet d'amorcer un apprentissage rapide.

Sous le système d'exploitation GNU/Linux il suffit d'installer GnuPG puis GPA depuis les dépôts de la distribution. Il y a d'autres interfaces graphiques proposées à l'usage, il suffit de faire son choix.

Sous Windows, on peut trouver un assortiment très intéressant : GPG4Win [26]. Il est maintenu par une administration allemande, l'Office fédéral de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik*). Il s'agit d'une suite logicielle (un choix est proposé lors de l'installation) contenant notamment :

— GnuPG : à installer si ce n'est pas déjà fait,
— GPA (GNU Privacy Assistant) : le gestionnaire de clés…
— Kleopatra : un autre assistant gestionnaire de clés qui permet notamment d'interagir avec le plugin GpgOL,
— GpgOL : un plugin qui s'installe dans Outlook et permet de signer, chiffrer et déchiffrer des courriels (à la manière d'Enigmail pour Thunderbird, dont nous parlerons plus tard).

25. `https://www.gnupg.org/`
26. `https://www.gpg4win.org/`

Le conseil est d'abord d'installer GPA et faire ses premières armes avec. Ensuite, les usages de Kleopatra et éventuellement le plugin pour Outlook vous seront facilement accessibles.

Dès l'ouverture de GPA, si vous n'avez pas encore de couple de clé privée / publique, le logiciel vous en proposera la création. Choisissez aussi de sauvegarder le jeu de manière à ce qu'à la fin du processus vous puissiez le stocker pour aussitôt le déplacer sur un support externe et le mettre en sûreté. Il est possible de lancer la procédure ultérieurement depuis le menu `Clé > Nouvelle clé`.

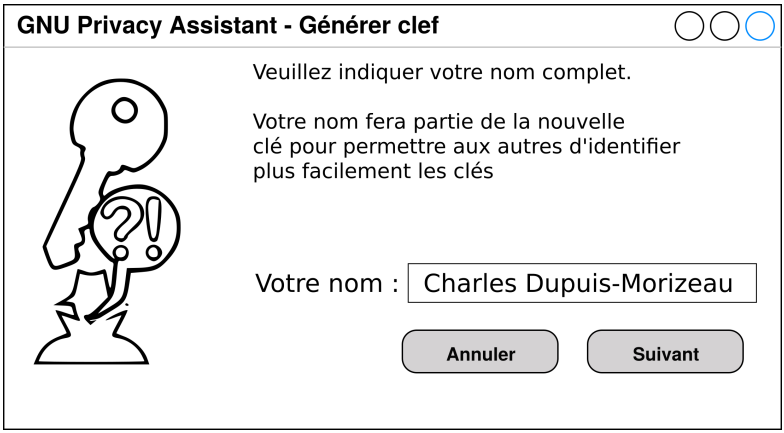


FIGURE 5.3 – Génération de clé avec GPA

Remplissez avec application les champs qui vous sont proposés, fenêtre après fenêtre :

— choisissez une adresse courriel dont vous êtes sûr de la validité (si vous voulez que cette clé puisse servir pour que l'on vous envoie des messages),
— choisissez votre nom ou un pseudonyme,
— choisissez une durée de validité de la clé (si vous êtes absolument sûr de vouloir l'utiliser indéfiniment),
— choisissez un mot de passe fort et surtout ne l'oubliez pas !

Toutes ces informations seront incluses dans le jeu de clés qui, une fois créé sera lui-même chiffré et stocké. Il est très important d'exporter ce nouveau jeu de manière à le stocker dans un endroit

sûr. Plus tard, lorsque vous serez plus à l'aise, vous pourrez générer des certificats de révocation et mettre des dates limites de validité sur vos clés.

Que faire ensuite avec GPA ? facile ! GPA propose un « presse papier », un petit éditeur de texte, qui vous permet d'écrire (ou coller) du contenu à chiffrer. De même, vous pouvez aussi ouvrir le gestionnaire de fichier pour choisir un fichier à chiffrer. GPA vous assiste alors : il suffit de choisir la clé publique avec laquelle vous désirez chiffrer le contenu et entrer le mot de passe de votre clé privée. Dans le cas d'un tampon de texte, GPA vous livre directement un contenu chiffré à copier et coller (par exemple dans un courriel) et dans le cas d'un fichier, GPA produit une copie chiffrée du fichier (qui se termine par l'extension `.gpg`).

Vous avez compris le principe ? et bien tous les assistants au chiffrement fonctionnent peu ou prou de la même manière. Comme GPA, il peuvent rechercher des clés sur un serveur de clés (avec les identifiants de clés), importer et exporter des clés, proposer une interface de chiffrement, etc.

Un serveur de clés

Si vous devez leur envoyer des contenus chiffrés, vous devez récupérer les clés publiques de vos correspondants. Soit vous leur demandez de vous les fournir en mains propres (sur une clé USB, par exemple) soit vous utilisez les services d'un serveur de clés où vous aussi vous entrerez vos clés publiques.

Voici un exemple de serveur de clés connu, hébergé par le MIT : MIT PGP Public Key Server [a].

Pour envoyer une clé vers un serveur, il vous faut d'abord exporter votre clé. La plupart des serveurs de clés publiques possèdent une interface pour enregistrer les clés publiques des utilisateurs. Vous pouvez toujours ajouter d'autres clés, mais en général, assurez-vous que votre clé est bien celle que vous utiliserez pendant longtemps ou bien pensez à la révoquer.

a. `http://pgp.mit.edu`

5.2.4.2 Chiffrer mes courriels

Certains assistants s'intègrent parfaitement dans des clients de courriel. C'est le cas de l'extension Enigmail[27] pour Thunderbird, que l'on installe depuis le catalogue d'extensions. Le tutoriel (en français)[28] présent sur le site *Surveillance Self Defense* de l'Electronic Frontier Fundation s'adresse aux utilisateurs de MSWindows, et traite d'une installation fraîche de GnuPG, Thunderbird et Enigmail. Pour les utilisateurs de GNU/Linux ou MacOS, les démarches sont similaires.

Pour résumer, Enigmail vous permet de configurer Thunderbird de manière à utiliser à la demande le chiffrement de vos courriels. Il permet, tout comme GPA, de créer des clés, stocker, importer, etc.

Avec votre téléphone portable sous Android, l'application OpenKeyCHain[29] vous permettra d'utiliser PGP tout aussi facilement que les logiciels cités ci-dessus. Le client de courriel K9-Mail (cf. chapitre 3) l'utilise par défaut, à l'image du couple Enigmail-Thunderbird. Mais OpenKeyCHain peut être utilisé indépendamment, y compris pour chiffrer des fichiers.

Enfin, puisque nous en avons parlé précédemment, le couple Kleopatra (un assistant à la manière de GPA) et GPGOL (une extension pour le client de courriel Outlook) sont inclus dans la suite Gpg4WIN. Les utilisateurs d'Outlook peuvent donc utiliser GnuPG sans problème avec ces deux outils.

5.3 Les mots de passe

Pourquoi utiliser des mots de passe ? Alors que nous pouvons chiffrer nos données et nos messages avec des clés, les mots de passe servent à protéger l'accès aux dispositifs, c'est-à-dire ouvrir des sessions. Ainsi, vous avez un mot de passe pour accéder à

27. https://addons.mozilla.org/fr/thunderbird/addon/enigmail/
28. https://ssd.eff.org/fr/module/pgp-sous-windows-le-ba-ba
29. https://www.openkeychain.org/

FIGURE 5.4 – Le chiffrement seul ne suffit pas toujours

votre messagerie, un mot de passe pour empêcher d'autres personnes d'utiliser votre ordinateur (à moins d'utiliser une session « invité »), un mot de passe pour chaque service web que vous utilisez, etc.

> **La complexité d'un mot de passe**
> Un « bon mot de passe » n'est pas une notion évidente. D'une part il doit être mémorisable, et d'autre part il faut y attacher un intérêt relatif à l'importance des données que l'on souhaite protéger. Ainsi certaines personnes jugent secondaire la complexité du mot de passe pour deux raisons : parce qu'elles craignent de l'oublier et parce qu'elles pensent que leurs données numériques n'ont aucune valeur (ce qui est fondamentalement faux).

Il y a plusieurs manières de pirater un mot de passe. La première consiste à tester des combinaisons une par une. On appelle cette méthode l'attaque par *force brute*. Elle nécessite un logiciel permettant d'automatiser très rapidement le traitement et les multiples essais. Si votre mot de passe est un mot présent dans un dictionnaire courant, de n'importe quelle langue, l'attaque durera quelques secondes. Plus longtemps si vous avez mis des chiffres.

Par contre, plus votre mot de passe sera long et complexe, plus il faudra de temps pour le découvrir et, au-delà d'une certaine limite, la procédure ne peut aboutir compte tenu des possibilités techniques actuelles (sauf pour les récentes avancées des ordinateurs quantiques). Par exemple,

UnmanchotvolantdansledesertduNevadalesoirdeNoel

sera plus difficile à craquer que `manchot25`. Mais pas impossible.

Une autre méthode pour découvrir un mot de passe est dite par « ingénierie sociale ». Elle consiste à établir le profil d'un utilisateur en fonction des informations qu'il a divulguées sur le web, notamment sur des réseaux sociaux. Ainsi, son nom, sa date de naissance, le nom de son chien, son adresse, etc. constitueront un ensemble de caractères pouvant être utilisés en priorité pour une attaque en force brute ou, plus simplement, pour élaborer des essais logiquement déduits par le pirate.

Par exemple : Monsieur Dupont a assisté à la naissance de son fils Kévin le 12/06/2003. Un mot passe probable pourrait être `kevin2003`.

5.3.1 Créer et utiliser les mots de passe

Il est conseillé de ne pas se contenter d'un simple mot composé uniquement de caractères alphabétiques `[a-z]`. Il vaut mieux utiliser une combinaison comprenant des caractères alphanumériques `[a-z, 0-9]`, des majuscules `[A-Z]` et des caractères spéciaux `[!,:@, etc.]`, le tout sur une longueur minimum de 10 caractères. L'idéal est de retenir une phrase de passe, qui excédera 10 caractères (des quatre types), et sera par conséquent plus facile à retenir.

Pour construire une phrase de passe, il faut aussi mémoriser la méthode de sa construction, sous peine de définitivement l'oublier. Plusieurs méthodes pourront vous aider :

— prenez une phrase et remplacez certaines lettres par d'autres caractères (et utilisez les 4 types de caractères mentionnés ci-dessus),

— utilisez la phonétique, par exemple : `GHT4dvdchez@t1t1!` (j'ai acheté 4 dvd chez @Tintin !),
— utilisez un générateur de mot de passe (le logiciel Keepass le permet, cf. plus bas).

Prenez quelques minutes pour vous inventer une méthode que vous n'oublierez pas. Un bien petit sacrifice pour la sécurité de vos données…

Dans tous les cas, respectez impérativement ces règles :

— utilisez un mot de passe différent pour chaque service auquel vous êtes inscrit-e,
— nettoyez le cache du navigateur après chaque utilisation et, par défaut, ne mémorisez pas le mot de passe dans votre navigateur,
— n'écrivez jamais votre mot de passe, même si on vous le demande : l'administrateur d'un site n'a jamais besoin de votre mot de passe pour effectuer des opérations sur le site,
— changez régulièrement de mot de passe.

5.3.2 Comment stocker mes mots de passe

En matière de pratiques comme de sécurité informatique, un adage connu affirme que le problème se situe souvent entre la chaise et le clavier. En effet, on ne compte plus les personnes qui stockent leurs mots de passe à l'aide de papiers collés sur l'écran ou sous le clavier. Il ne faut pas oublier beaucoup d'intrusions informatiques se font grâce à un accès physique aux machines, en particulier lorsque des ordinateurs se trouvent dans des endroits publics, ou même dans un bureau, et bien sûr en cas de vol. Il faut donc rester vigilant.

Heureusement d'autres moyens sont à votre disposition : les logiciels gestionnaires de mots de passe. Attention : beaucoup de solutions logicielles existent sur le marché, il faut savoir évaluer leur degré de confiance. Il existe trois types de solutions :

1. des logiciels / applications propriétaires. À moins que votre entreprise en ait fait l'audit et vous oblige à en utiliser une, ne faites pas confiance à ces logiciels tant que vous n'en n'avez pas l'expertise ;

2. des services en ligne. Là aussi, vous devez non seulement faire confiance aux technologies employées, mais elles sont de plus, et par définition, vulnérables à de nombreuses attaques (quel pirate ne rêve pas de s'attaquer à un site qui prétend regrouper les données d'accès de milliers d'utilisateurs ?) ;
3. des solutions logicielles libres, qui non seulement font l'objet d'audits permanents de la part des utilisateurs (du moins ceux qui en ont l'expertise), mais qui, de surcroît jouent la transparence en publiant leur code source.

Pour cette troisième catégorie, il est aussi plus facile de se renseigner sur les audits. Ainsi, l'un des logiciels les plus plébiscités dans ce domaine se nomme Keepass [30] (Keepass Password Safe). C'est un logiciel libre qui a de plus été passé au crible [31] par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et bénéficie d'une Certification de Sécurité de Premier Niveau (CSPN). La CNIL mentionne Keepass [32] sur une page consacrée aux mots de passe dont vous pouvez bénéficier de la lecture.

Keepass a d'abord été développé pour Windows. Dans sa version GNU/Linux, il se nomme KeepassX [33], un portage de Keepass. L'utilisation est très simple. Il s'agit d'une base de données dotée d'une interface pour remplir différents champs (titre, nom d'utilisateur, mot de passe, etc.). Il est possible de spécifier une date d'expiration pour chaque entrée.

La base de données est sauvegardée dans un fichier d'extension `.kdbx` et dotée d'une phrase de passe. Cette dernière est alors suffisante pour ouvrir la base et récupérer ses mots de passe. Cela permet à l'utilisateur de n'avoir à retenir qu'un seul mot de passe pour tous les autres. Bien sûr ce mot de passe devra être bien complexe et le fichier de la base stocké dans un endroit difficile d'accès.

30. `http://keepass.info/`
31. `https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/`
32. `https://www.cnil.fr/fr/construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces`
33. `https://www.keepassx.org/`

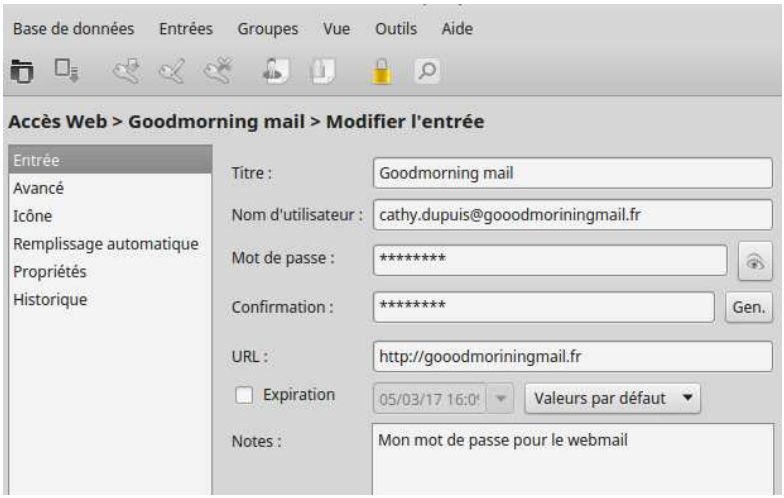


FIGURE 5.5 – Entrée de données dans Keepass

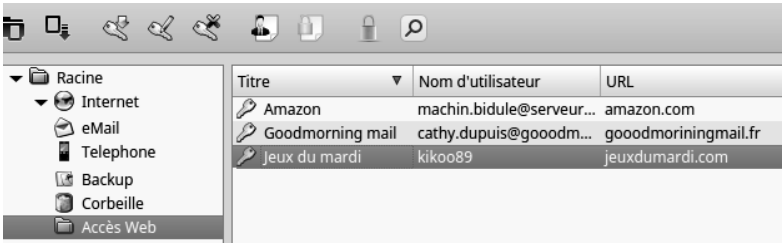


FIGURE 5.6 – Interface de Keepass

Beaucoup d'extensions (plugins) sont disponibles. Elles permettent par exemple d'interfacer Keepass avec son navigateur, de synchroniser Keepass avec d'autres appareils comme un smartphone, ou encore de synchroniser la base de données avec un stockage en ligne (déconseillé sauf pour un usage peu sensible).

Du côté des appareils mobiles, l'application Keepassdroid [34] (mentionnée sur le site PrismBreak [35]) est un port de Keepass sur plate-forme Android et permet donc d'utiliser des fichiers `.kdbx`. Avec un peu de pratique, il est alors possible d'ouvrir la même base de donnée sur votre mobile et sur ordinateur, ce qui vous permet de la transporter avec vous. Toutefois, votre prudence est de mise : les appareils mobiles sont des dispositifs très sensibles au niveau de la sécurité et du chiffrement.

5.4 Surfer en sécurité

Comme nous l'avons vu avec PGP, il est important de bien comprendre que sur le réseau, lorsque deux machines communiquent entre elles, il faut leur demander explicitement de le faire de manière chiffrée. En fait, lorsque vous surfez sur le web, vous utilisez des protocoles qui permettent par exemple à votre navigateur d'envoyer et recevoir des informations et les afficher. C'est le cas d'usage du HTTP (HyperText Transfert Protocol). Or, selon les besoins, surtout lorsque vous consultez un site dont les données sont sensibles (votre compte en banque, vos données de santé, votre messagerie en ligne, etc.) il est important d'ajouter un protocole de sécurité en plus : SSL (Secure Socket Layer).

5.4.1 Le HTTPS : pourquoi ?

SSL est une couche (layer) supplémentaire aux protocoles habituels qui permet d'amorcer une session sécurisée de transmission

34. `http://www.keepassdroid.com/`
35. `https://prism-break.org/fr/projects/keepassdroid/`

entre deux machines. Lorsque vous surfez et que vous voyez apparaître l'occurrence `https` au lieu de l'habituel `http` dans la barre d'adresse, c'est que la connexion s'établit, en plus, sur une base SSL. Très rapide et pratiquement invisible aux yeux de l'internaute, une connexion SSL se déroule en deux temps (deux protocoles) :

— une phase de négociation (SSL Handshake protocol) : les deux machines négocient des clés de chiffrement et s'accordent sur les protocoles d'échange,

— la phase d'échange (SSL Record protocol) : les deux machines communiquent et contrôlent les échanges.

Comme dans le cas de l'utilisation de PGP, le chiffrement est asymétrique (échange de clés) et utilise un système de signature visant à contrôler l'intégrité des informations de l'émetteur au récepteur (s'assurer que personne n'a intercepté l'information pour la renvoyer modifiée).

Un concept très important dans le cas de connexion SSL, c'est le certificat. Lors de la phase de négociation, les deux machines échangent des certificats, c'est-à-dire des pièces d'identité. Lorsque vous vous connectez à votre banque, que vous ayez un certificat ou non importe peu : l'essentiel est que votre banque, elle, en ait un qui puisse l'authentifier de manière à être sûr-e que c'est bien sur le site de votre banque que vous vous trouvez et avec qui vous allez échanger des informations.

Là encore, ce n'est pas l'utilisateur qui, manuellement, doit s'assurer de l'authenticité du certificat émis par le correspondant. En fait, chaque navigateur dispose d'une liste d'autorités (des PKI, Public Key Infrastructure) auxquelles il s'adresse et qui vont endosser cette authentification. Ces autorités sont des organismes agréés (sociétés de droit privé ou institutions publiques) qui disposent d'un ensemble de dispositifs informatiques et humains de certification.

Si le navigateur ne parvient pas à faire le lien entre une autorité et le certificat reçu, il prévient l'utilisateur, notamment avec un jeu d'icônes. Dans le cas du navigateur Firefox[36] les icônes en forme de cadenas correspondent à plusieurs cas de figure[37] :

36. `https://www.mozilla.org/fr/firefox/desktop/`

37. `https://support.mozilla.org/fr/kb/comment-savoir-si-ma-connexion-est-securisee`

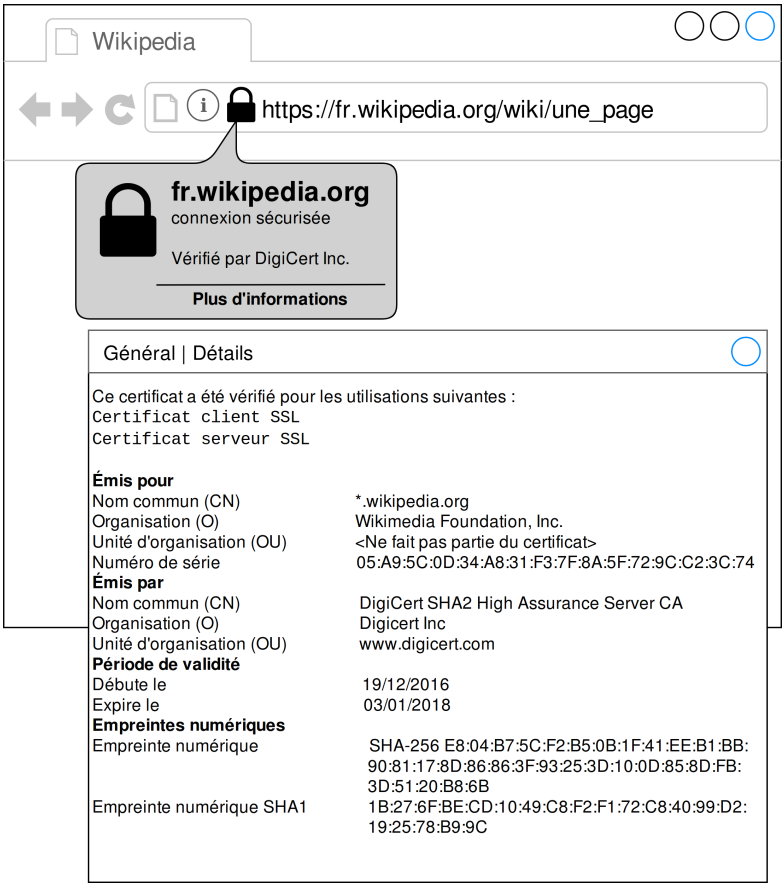


FIGURE 5.7 – Exemple de certification authentifiée sur le site Wikipédia

— une simple information qui prévient que le site n'est pas certifié (mais comme n'y a pas lieu d'y entrer des informations, l'absence de formulaire, etc. il n'y a pas d'alerte) ;
— une alerte signifiant que le site n'est pas authentifié, que la communication n'est pas chiffrée, et que tout ce qui pourra y être communiqué par l'utilisateur risque d'être intercepté ;
— un avertissement indiquant que le site, bien qu'authentifié, contient des éléments qui ne sont pas sécurisés et que la communication n'est que partiellement chiffrée ;
— une indication qui atteste que la communication est entièrement chiffrée et le site certifié.

En d'autres termes, lorsque vous vous rendez sur un site où vous êtes censé entrer des informations, confidentielles ou non, ayez toujours un œil en haut à gauche de la fenêtre de votre navigateur !

5.4.2 L'affaire des cookies

Dans le jargon informatique, un cookie[38] est un moyen de formaliser une transaction entre deux programmes, le plus souvent par un fichier qui fait office de jeton. Il s'agit d'un *témoin de connexion* qui atteste la connexion d'une machine à une autre. Les cookies existent depuis très longtemps dans l'histoire de l'informatique moderne mais l'omniprésence des réseaux a multiplié leur usage.

Concrètement, un cookie est un fichier texte stocké sur la machine de l'internaute (généralement dans un emplacement désigné et utilisé par le navigateur) et qui retourne des informations lorsque le serveur les lui demande. Par exemple, lorsque vous faites des achats sur une boutique en ligne, un cookie contenant des identifiants ou un code généré en fonction des identifiants de connexion, vous permet de gérer votre panier d'achat en renvoyant ce cookie qui vous identifie sur le serveur à chaque fois que vous y ajoutez quelque chose ou lorsque vous voulez payer.

Les cookies sont donc des dispositifs fort utiles. Ils sont là au départ pour permettre d'ouvrir et fermer une session d'utilisation

38. `http://www.catb.org/~esr/jargon/html/C/cookie.html`

d'un site web ou de tout autre service. Cependant, ils peuvent emmagasiner bien d'autres informations, notamment à des fins de marketing mais qui peuvent mettre en danger vos informations personnelles et votre confidentialité.

5.4.2.1 Cookies et sécurité

Un cookie n'identifie pas l'utilisateur derrière le clavier, mais le navigateur sur votre machine se connectant à un serveur distant. Fermer une session sur un site distant ne signifie donc pas forcément que le cookie qui vous permettait de vous identifier est nettoyé de ces informations. Si une personne utilise votre machine et votre navigateur après vous, il y a des chances qu'elle puisse accéder à des informations non souhaitées.

Voici un scénario probable : en prévision de la Saint Valentin, vous effectuez des achats en ligne pour faire une surprise à votre conjoint-e. Un cookie va alors stocker la valeur totale de vos achats. Une fois les achats effectués, votre conjoint-e utilise à son tour le navigateur pour se rendre avec la même intention sur le même site… et voit s'afficher le montant de votre dernière transaction.

Ce dernier scénario issue de la vie domestique peut prêter à sourire, mais les conséquences ne sont pas toujours négligeables : certains cookies, ajoutés à votre historique de navigation, vous permettent même de retourner des informations d'identité pour ne pas avoir à saisir votre numéro de carte bleue lors des achats ultérieurs. Or, les autres utilisateurs de la machine (autorisés ou pas) ne sont pas toujours des personnes bien intentionnées…

Un autre exemple de vulnérabilité concerne l'interception de cookies. Un tiers peut en effet s'interposer entre votre navigateur et le serveur, ou bien ce dernier peut lui-même avoir été piraté. Dès lors, il est possible que votre session soit détournée et que toutes les informations que vous retournez avec les cookies soient récupérées. Ce détournement de session est une pratique qui peut être contrée par la protection SSL et le chiffrement de session, ce que nous avons vu précédemment à propos de HTTPS. Cependant, même si la connexion entre le serveur et le client est chiffrée, la durée d'existence d'un cookie dans votre navigateur peut parfois être

de plusieurs jours et excéder la durée de la connexion, ce qui cause une réelle faille de sécurité pour vos données privées en fonction des sites sur lesquels vous vous rendez.

5.4.2.2 Les cookies et ma vie privée

La directive européenne du 25 novembre 2009 (modifiant la directive 2002/22/CE – directive « service universel ») indique :

> Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement.

On comprend que dans ces conditions l'usage des cookies devrait être réservé à l'amélioration des services et de l'expérience utilisateur. Cependant, dans la mesure où les cookies servent surtout à mesurer des parts d'audience et les comportements des utilisateurs, beaucoup de sites font en réalité appel à des sociétés spécialisées. Dans d'autres cas, des grands acteurs de services, tels Facebook, offrent grâce à leur notoriété de quoi augmenter l'envergure de leurs services en proposant à d'autres sites de les relayer. C'est le cas, par exemple, lorsque le site d'un quotidien permet de « liker » un article avec un bouton Facebook : cela permet d'augmenter l'audience du journal en relayant l'article sur Facebook et cela permet à Facebook de mesurer le comportement de ses utilisateurs pour leur offrir une « meilleure expérience » en leur proposant des contenus similaires.

Ces procédés qui consistent à user et abuser de cookies issus de tierces parties ouvrent de plus vastes questions sur la vie privée. Si je me rends sur un site, je ne m'attends pas forcément à ce qu'un tiers fasse le lien entre cette visite et un autre site. Un même

émetteur est ainsi capable de recouper les informations issues de plusieurs sites sur lesquels se rend l'utilisateur. Ces analyses comportementales permettent d'inférer des profils à l'insu des utilisateurs. Cela fait des cookies non plus des instruments au service de l'expérience technique de l'utilisateur, mais de véritables mouchards. C'est pourquoi certains pays ont tenté d'adopter une législation stricte en la matière.

5.4.2.3 Surveiller les cookies que je reçois

Comme nous l'avons vu, si tous les cookies ne sont pas amicaux, le principe ne doit néanmoins pas être rejeté en bloc. Une bonne pratique, qui ne nécessite pas de compétences particulières, consiste à nettoyer son navigateur une fois que la session est terminée. Pour ce faire, une fonctionnalité de votre navigateur vous permet de supprimer l'historique, cookies compris, de manière ponctuelle ou de manière systématique. N'hésitez pas à employer cet outil.

Une autre manière de surveiller les cookies, consiste à paramétrer son navigateur. Par défaut, un navigateur comme Firefox accepte les cookies, y compris les cookies de tierce partie. Il est donc possible de les bloquer systématiquement en se rendant dans Firefox : `Préférences > Vie privée`.

Une autre méthode consiste à surfer en utilisant des fenêtres de navigation privée (en cliquant sur le petit masque ou en faisant `CTRL+Maj+P`). Le mode de navigation privée protège contre le pistage [39] et n'enregistre pas d'historique.

En 2014, l'Electronic Frontier Foundation (EFF) s'est penché sérieusement sur le problème des cookies. L'EFF est une organisation non gouvernementale et à but non lucratif, qui vise à défendre la liberté d'expression sur Internet. Son rôle se compose à la fois de veille, d'alerte et de pédagogie. Dans la mesure où l'usage déloyal des cookies menace nos intimités numériques, l'EFF a développé une extension pour Firefox et Chrome nommée Privacy Badger [40].

39. `https://support.mozilla.org/fr/kb/protection-contre-le-pistage-en-navigation-privee`
40. `https://www.eff.org/fr/privacybadger`

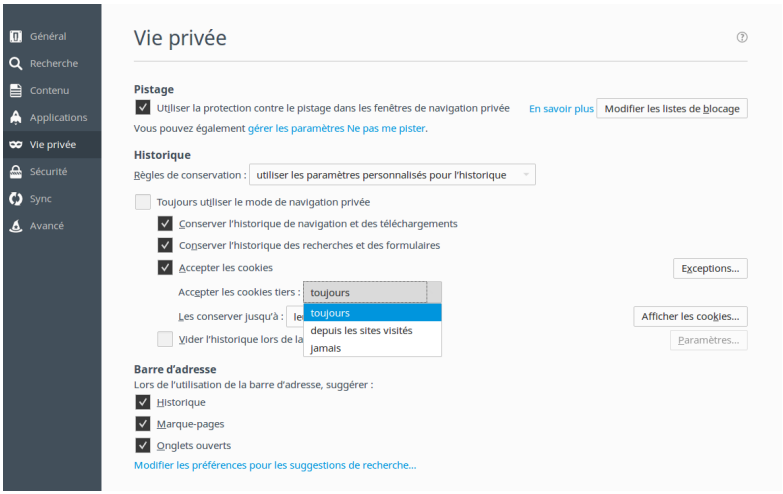


FIGURE 5.8 – Surveiller les cookies avec Firefox

Cette extension, installable en un clic sur votre navigateur, permet de monitorer et bloquer les cookies. Son but général est à terme d'obliger les émetteurs à respecter la fonction *do not track* (DNT — une fonction du navigateur [41] qui indique que l'utilisateur ne souhaite pas être pisté).

La page Wikipédia consacrée à Privacy Badger [42] explique en quelques mots simples le fonctionnement de Privacy Badger :

> Privacy Badger ne fonctionne pas à partir d'une liste toute faite de sites à bloquer (liste noire) mais utilise un algorithme pour détecter dynamiquement des comportements de pistage par des sites tiers. Cette approche heuristique présente deux avantages : actualité (par la technique de l'apprentissage automatique la contre-mesure est toujours à jour), impartialité (pas de pressions tierces concernant le contenu d'une liste centralisée pré-établie).

41. `https://support.mozilla.org/fr/kb/comment-activer-option-ne-pas-pister`
42. `https://fr.wikipedia.org/wiki/Privacy_Badger`

Lors de la visite d'un site, le navigateur web charge automatiquement des contenus de différents sites tiers : Privacy Badger recense ces sites. Puis, si au cours des pérégrinations en ligne ultérieures, les mêmes sites semblent pister la navigation sans autorisation, alors Privacy Badger entre en action en demandant au navigateur de les bloquer. Et comme le navigateur ne charge plus rien en provenance de ces sites, ils ne peuvent plus pister l'internaute.

FIGURE 5.9 – Usage de Privacy Badger sur un site connu

5.5 Et mon anonymat ?

De manière synthétique, Eben Moglen [43] exprime en une phrase tout le problème de nos intimités numériques sur Internet : « nous n'avons pas inventé l'anonymat lorsque nous avons inventé Internet » [44]. En effet, aux fondements d'Internet, c'est le partage de l'information qui prime. La surveillance des utilisateurs n'est qu'une conséquence d'un usage déloyal des protocoles utilisés pour partager l'information.

Dès lors, l'anonymat prend une autre dimension. Il n'est plus seulement l'ignorance ou la dissimulation de l'identité. Car ce qui définit justement notre identité sur Internet, ce n'est pas notre présence administrative c'est l'ensemble des comportements et des traces numériques qui sont analysées, recoupées, inférées, de manière à profiler notre identité et celle de nos correspondants. Ces usages sont devenus tellement automatiques que beaucoup d'internautes sont prêts à sacrifier une partie de leurs droits à l'image pour pouvoir utiliser un service gratuit (voyez les conditions d'utilisation de Facebook qui s'approprie vos données biométriques et pratique des analyses de reconnaissance faciale [45]). Mais l'enjeu est encore plus large : la raison pour laquelle nous devons protéger nos accès aussi bien que notre identité numérique, c'est d'abord et avant tout pour protéger ceux avec qui on échange. Car tout l'intérêt de l'analyse des données, ce n'est pas le contenu de votre dernier message à votre ami à l'autre bout du pays, c'est la fréquence de ces échanges, les lieux et les durées, et ce sont ces données qui intéressent avant tout les firmes pour des raisons de marketing et

43. Eben Moglen est professeur de droit et d'histoire du droit à l'université Columbia, président du Software Freedom Law Center, et avocat conseil à la Free Software Foundation.

44. Voir cette conférence (traduction sous-titrée) de Eben Moglen, « Why Freedom of Thought Requires Free Media and Why Free Media Require Free Technology », *Re :Publica*, Berlin, 02/05/2012.

45. Pour plus d'information, voir les articles suivants. Tom Simonite, « Facebook Creates Software That Matches Faces Almost as Well as You Do », *MIT Technology Review*, 17/03/2014. Dino Grandoni, « DeepFace, le nouveau système de reconnaissance faciale de Facebook qui fait froid dans le dos », *Le Huffington Post*, 20/03/2014. Dépêche AFP/Le Figaro, « Facebook devant la justice pour sa technologie de reconnaissance faciale », *Le Figaro*, 06/05/2016.

les programmes de surveillance de certains États (qui impliquent ces mêmes firmes [46]).

Anonymat ou confidentialité ?

Attention toutefois à ne pas confondre l'anonymat et l'impossibilité d'être identifié. Quoi que vous fassiez sur Internet, il est impossible de masquer totalement un ou plusieurs éléments qui permettent de remonter à la source. Pour différencier les données, il faut bien fatalement que votre machine soit identifiée sur le réseau. À vous de faire en sorte que l'identité technique de votre machine soit distincte de votre identité administrative. On préfère donc parler de *confidentialité* sur Internet.

5.6 Utiliser TOR

TOR est l'acronyme de The Onion Router. Il s'agit d'abord d'un réseau qui fonctionne par nœuds qui « répercutent » les connexions des utilisateurs. Ainsi, tout comme les couches des pelures d'oignon, si on identifie un nœud par lequel l'utilisateur est passé, c'est à un autre nœud qu'il renvoie, etc. Le réseau TOR est donc décentralisé. Pour fonctionner, la liste des nœuds étant publique, il connecte les utilisateurs sur ces nœuds et construit des routes (un routage) qui leur permettent de surfer sur Internet mais en passant par différents nœuds à chaque fois. Le site visité ou tout autre acteur ne peut donc pas identifier la provenance exacte de l'utilisateur, à moins d'utiliser des outils spécifiques d'analyse en profondeur du réseau et vous rechercher activement.

Pour assurer cette confidentialité pour toutes sortes de connexion Internet, il faut configurer son système d'exploitation

46. Si vous pensez ne rien avoir à cacher, vous pouvez regarder cette vidéo par Julien Vaubourg (Lorraine Data Network), « Je n'ai rien à cacher [47] », séminaire MathC2+, à Inria Grand Est, 14/04/2015.

avec les données du réseau TOR. C'est une pratique plutôt fastidieuse. C'est pour cette raison qu'il existe TAILS [48] (The Amnesic Incognito Live System), une distribution GNU/Linux entièrement paramétrée pour cela. TAILS n'est pas censée obligatoirement s'installer sur votre disque dur à la place de votre système d'exploitation actuel. C'est d'abord une distribution « live », c'est-à-dire qu'elle s'installe sur une clé USB ou une carte SD et vous permet de disposer ainsi d'une session à la demande, non seulement pour surfer, mais aussi pour disposer d'un panel d'outils dédiés au chiffrement.

De manière moins complexe, il existe un navigateur développé par le projet Tor, sur la base de Firefox : Tor Browser Bundle [49]. Pour résumer, ce navigateur s'installe et s'utilise de la même manière qu'un navigateur classique, à la différence qu'il se connecte d'abord au réseau TOR et que vous pouvez configurer le niveau de sécurité avec un curseur. Si vous utilisez Windows, vous pouvez vous reporter à cette page d'explication [50] pour installer et configurer Tor Browser. La seule condition pour utiliser Tor Browser correctement, c'est de toujours disposer de la dernière version à jour.

Pour conclure sur l'utilisation de TOR, il est important de préciser que cet outil n'est pas destiné à effectuer des opérations illicites. Il est d'abord construit de manière à respecter la confidentialité des utilisateurs. Il n'est donc pas forcément pertinent de l'utiliser à tout bout de champ, dans un délire paranoïaque permanent, même si dans certains pays son utilisation (couplée à d'autres dispositifs encore) est d'abord une question de liberté d'expression et de survie. L'utilisation de TOR se fait à bon escient, car rien ne remplacera votre attention et votre bon sens.

48. https://tails.boum.org/
49. https://www.torproject.org/projects/torbrowser.html
50. https://ssd.eff.org/fr/module/guide-dutilisation-de-tor-pour-windows

Conclusion

Nous sommes tous des DuMo. Qui pense tous les jours à chiffrer ses communications avec PGP ? Avons-nous tous envie de changer nos vieilles habitudes ? Qui est prêt à abandonner du jour au lendemain un logiciel avec lequel il a déjà pris ses marques ?

Comme tout guide de bonnes pratiques, celui-ci n'a certes pas l'ambition d'être exhaustif ni d'imposer des usages. Il montre que si des alternatives aux logiciels propriétaires existent, le seul fait de les utiliser ne suffit pas à garantir les libertés numériques que tout le monde est en droit d'exiger. Si vous gardez votre compte Facebook, vous êtes en droit de le faire, surtout si c'est votre seul moyen de conserver vos contacts avec les gens que vous aimez. Vous pouvez aussi continuer à utiliser GMail parce que son ergonomie vous plaît. Mais au moins, après cette lecture, vous comprenez les enjeux que soulèvent ces services numériques gratuits face à votre intimité numérique. Vous comprenez aussi que même en les utilisant, certains réflexes sont nécessaires comme le fait d'utiliser des protocoles sécurisés avec un client de courriel ou de vérifier les cookies que votre navigateur engrange au fil des pages visitées.

Petit à petit vous reprendrez les clés de lecture que vous offre cet ouvrage. Elles vous serviront pour analyser vos pratiques, les

mésaventures de vos amis et vos propres difficultés. Chaque chapitre, chaque section mériterait un développement bien plus complet et rigoureux, jusqu'à atteindre les 15 tomes nécessaires pour faire de vous un-e vrai-e guerrier-e numérique. C'est peut-être le grand défaut des spécialistes que d'exiger du néophyte une attention de tous les instants. C'est ce qui a sans doute lassé Madame Michu.

Alors, non. Ne retenez pas par cœur toutes les définitions de cet ouvrage. Ne répétez pas religieusement tous les soirs les quatre libertés du logiciel libre. Ne saturez pas vos voisins d'affirmations péremptoires sur les dangers de la surveillance de masse.

Refermez ce livre et rangez-le. Mais pas trop loin. Vous savez maintenant identifier et évaluer vos besoins en termes d'outils, d'applications et de méthodes. Vous vous souviendrez de quelques noms de logiciels que vous finirez par installer pour toutes les bonnes raisons du monde. Vous finirez par vous libérer. Et c'est tout naturellement que vos amis en feront autant, simplement parce que vos usages protègent aussi leurs libertés. Si ! vous verrez… cela commence déjà.

ANNEXE A

Glossaire

Application Programme (logiciel) destiné à l'utilisateur et servant à réaliser des tâches dans un domaine particulier (traitement de texte, navigation web, etc.). Pour ne pas confondre application et logiciel, voyez « Logiciel », plus loin dans le Glossaire.

Chiffrement Un procédé (de cryptographie) qui rend impossible la compréhension d'un message sans une clé de déchiffrement.

Client (logiciel) Un logiciel client est un logiciel qui permet de communiquer avec un serveur et de récupérer ou envoyer des données selon des protocoles définis. Un client de messagerie électronique est un logiciel qui récupère et envoie des messages électroniques sur un serveur selon les protocoles IMAP, POP, Exchange, etc.

Cookie Un témoin de connexion qui fait office de jeton afin d'authentifier ou attester la connexion entre deux machines. Un cookie peut aussi véhiculer d'autres informations.

Cracker Un amateur ou un expert spécialisé dans le cassage des protections de sécurité des logiciels.

Cryptographie Art (ou discipline) de protéger des messages en les rendant inintelligibles, notamment au moyen du chiffrement.

Dépôt (logiciels) Un dépôt est un service de stockage et diffusion de logiciels. Pour les utilisateurs de GNU/Linux, chaque distribution propose des dépôts validés. On s'y connecte via un gestionnaire de dépôts afin de télécharger et installer les programmes que l'on souhaite. Si un logiciel ne se trouve pas dans les dépôts, c'est qu'il n'a pas encore été validé ou qu'il ne présente pas les caractéristiques suffisantes de stabilité et de sécurité. Selon votre système d'exploitation, les dépôts sont parfois appelés *store* ou *magasin*.

Distribution Une distribution est un ensemble cohérent de logiciels permettant d'effectuer un ensemble de tâches spécialisées. Les différentes versions de systèmes d'exploitation GNU/Linux sont des distributions : elles répondent à des besoins différents, ne proposent pas toutes les mêmes logiciels.

Extension (fichier) Quelques caractères à la fin d'un nom de fichier, après un point, servant à identifier rapidement le format du fichier.

Extension (logiciel) Une extension ou un *module* d'extension ou encore un *plugin* est une série de commandes se greffant à un logiciel *hôte* afin d'étendre ses fonctionnalités.

Format (fichier) Un format de fichier est une convention qui représente la manière dont sont arrangées et stockées les données regroupées dans ce fichier.

Hacker Un passionné d'informatique, qui apprécie notamment de bidouiller en vue d'améliorer des programmes ou du matériel.

Internet Un réseau informatique mondial accessible au public. Les échanges s'y font grâce à des protocoles standards de communication.

Interopérabilité (des formats) L'interopérabilité d'un format de fichier est sa capacité à fonctionner ou être traité par des logiciels différents.

Libre (logiciel) Un logiciel libre est un logiciel placé sous une licence qui respecte les quatre libertés logicielles : 1. la liberté d'utiliser le logiciel, 2. la liberté de copier le logiciel, 3. la liberté d'étudier le logiciel, 4. la liberté de modifier le logiciel et de redistribuer les versions modifiées.

Licence libre Un contrat qui formalise l'exercice des quatre libertés logicielles (lorsqu'il s'agit d'un logiciel libre) ou qui s'inspire de ces quatre libertés pour contractualiser l'usage d'un contenu ou d'une œuvre.

Logiciel Ensemble d'instructions (programme(s)) et jeu de données (fichiers) qu'un utilisateur ou une machine utilise pour effectuer des tâches. Un logiciel de traitement de texte est un programme qu'on peut qualifier d'applicatif (voir « Application »). Un noyau de système d'exploitation est un programme qui n'a pas une visée applicative.

Navigateur (Web) Un navigateur est un logiciel permettant d'afficher le Web, en particulier en utilisant le protocole HTTP.

Nétiquette Ensemble de règles informelles visant à structurer les bonnes pratiques d'usage de la messagerie entre internautes.

Noyau (système d'exploitation) Un noyau est un programme à la base du système d'exploitation. Il permet de gérer les accès aux dispositifs de calcul et de mémoire, coordonne les programmes et les éléments matériels. Linux est le noyau d'un système GNU/Linux.

Piratage Action illégale dans le domaine informatique : contrefaire des œuvres, s'approprier des données, usurper des identités etc.

Port (matériel) Une prise permettant de brancher un périphérique sur un ordinateur.

Port (logiciel) Un système permettant de gérer les entrées et sorties d'information.

Propriétaire (ou privateur) Un programme est dit propriétaire s'il ne permet pas l'exercice des 4 libertés propres au logiciel libre. La principale caractéristique est la non diffusion du code source et l'impossibilité d'un audit public du logiciel. Il constitue donc une porte ouverte pour un usage déloyal des données des utilisateurs qu'il traite. C'est pour cette raison que le terme « privateur » (de libertés) est aussi employé.

Protocole de communication Une suite d'opérations nécessaires pour mettre en relation deux machines sur un réseau. Un protocole peut intégrer le procédé de mise en relation, la convention d'échange, le contrôle de la communication.

RFC *Request for comment* : ce sont des documents officiels rédigés sur la base de commentaires calibrés et servant à décrire les aspects techniques d'internet après délibération. Certaines RFC sont devenues des standards.

Système d'exploitation Un ensemble de programmes qui permet d'exploiter les ressources d'un ordinateur (matériel, surtout).

Virus (informatique) Un programme qui se propage d'un ordinateur à l'autre. Il peut contenir du code malveillant qui agit par exemple en supprimant des données ou en les chiffrant (pour permettre à ses commanditaires de réclamer une rançon en échange de la clé de déchiffrement).

Web (World Wide Web) C'est le système hypertexte fonctionnant sur le réseau Internet, grâce à un navigateur qui permet de récupérer des contenus. L'image de la toile (*web*) est employée pour illustrer les liens hypertextes qui lient les pages entres elles.

Webmail Un client de messagerie électronique disposant d'une interface Web permettant de gérer son courrier en ligne à l'aide d'un navigateur.

Table des matières