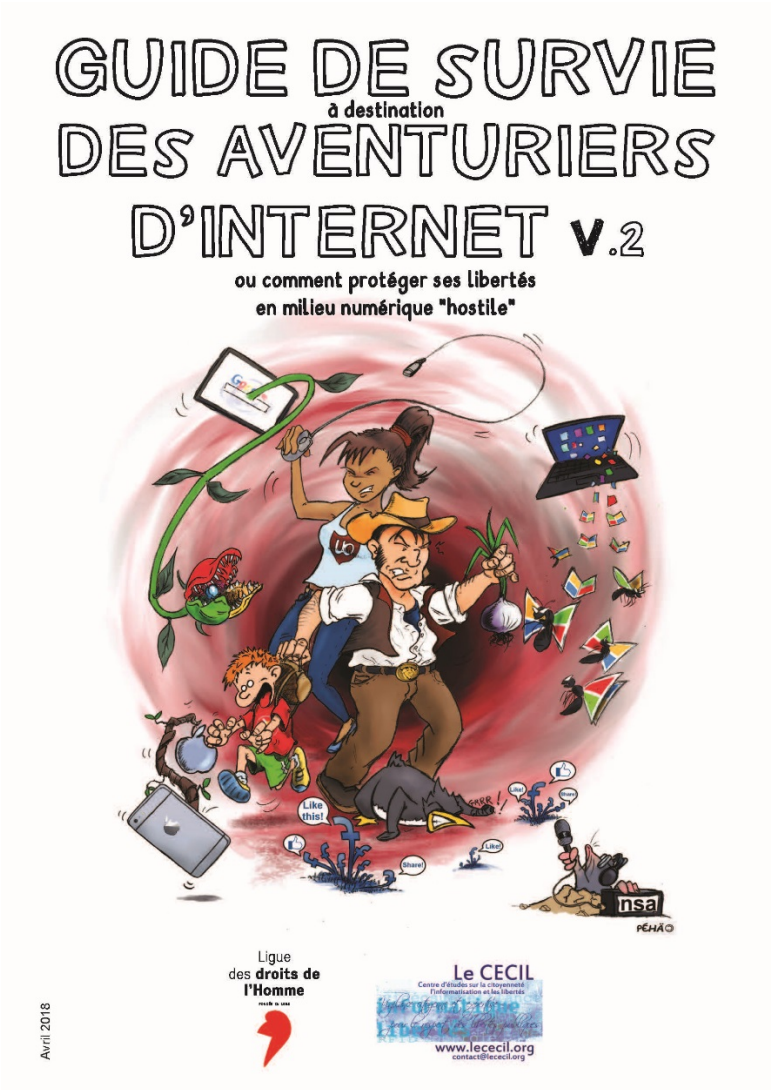
Les fiches pratiques du CECIL pour défendre ses libertés face à la surveillance en ligne

Le CECIL
Centre d'études sur la citoyenneté l'informatisation et les libertés
Vigilance citoyenne et expertise pour le respect des libertés publiques
www.lececil.org
contact@lececil.org

Ces fiches pratiques ont été éditées sous forme d'un guide papier disponible à la vente, pour plus d'informations cliquer sur ce lien et pour directement le commander sur Helloasso c'est par là.



Introduction

Les multiples révélations d'Edward Snowden concernant les dérives des programmes de surveillance de la NSA ont bien montré que les États-Unis et leurs alliés (mais ce ne sont malheureusement pas les seuls) écoutent et traitent massivement les informations de gouvernements étrangers, d'entreprises et d'individus (majoritairement non américains) souvent par l'intermédiaire de compagnies telles que Microsoft, Yahoo, Google, Facebook, AOL, Apple… En plus de cette surveillance étatique, une personne peut aussi être la cible d'entreprises commerciales et de pirates informatiques mal intentionnés. Conformément à son objet social de protection des individus face aux risques de l'informatique, le CECIL propose un recueil de fiches pratiques pour découvrir, pas à pas, des outils visant à mieux maitriser les informations exposées, protéger la vie privée et les libertés fondamentales. Il ne s'agit pas ici d'être exhaustif, mais de faire (re)découvrir à la personne inquiète, quoique peu connaisseuse, une sélection de techniques de base. À la fin de chaque fiche, des références complémentaires sont indiquées. Ces fiches proposent l'utilisation de logiciels respectueux de la vie privée, en complément de bonnes pratiques.

Présentations des fiches

1. Le système d'exploitation et le navigateur : deux outils fondamentaux

L'achat d'un ordinateur, ou même d'un ordiphone (smartphone), se fait souvent essentiellement en fonction de caractéristiques matérielles, alors que les éléments logiciels de base sont rarement pris en compte. Il en est ainsi du système d'exploitation (Windows ou Mac OS X) et du navigateur installés par défaut (non choisi), facturés insidieusement dans le prix total. Il reste tout de même possible de remplacer ces logiciels installés par défaut. Il existe des alternatives bien plus respectueuses des libertés, gratuites et tout aussi fonctionnelles. Ce sont les "distributions" Gnu-Linux telles que Linux Mint pour le système d'exploitation ou Firefox pour le navigateur.

2. Les logiciels libres

Face aux grands éditeurs dits "propriétaires" (Microsoft, Apple, Adobe…) nombreuses sont celles et ceux qui ont fait l'effort de mettre au point des logiciels dits "libres" sur des fondements de partage de la connaissance et du respect des libertés. Ces logiciels garantissent l'usage de standards et de grandes libertés d'utilisation, d'étude, de redistribution et d'amélioration du programme. Cela permet notamment d'auditer le code et ainsi de limiter des possibilités malicieuses (portes dérobées, contrôle par un éditeur commercial…). En conséquence, la "communauté" exerce un fort contrôle sur ces logiciels. Dans une société où l'informatique est omniprésente, la maitrise de nos outils est un enjeu majeur. Les militant·es du logiciel libre participent à ce combat.

3. Les moteurs de recherche alternatifs

Les moteurs de recherche (Google, Yahoo…) servent de porte d'entrée à la découverte de la multitude d'informations et contenus sur Internet. Ce sont des acteurs clés du Web et certains en profitent pour enregistrer les données sur les recherches effectuées par les personnes et les tracer. Au-delà de l'établissement de profils individuels, ils disposent ainsi d'informations sur les idées, comportements et pratiques des populations. Cela est susceptible de représenter un danger sérieux pour la vie privée de tous et l'équilibre de la société. La fiche "Moteurs de recherche alternatifs" présente des moteurs qui ont une politique plus respectueuse des libertés. C'est par exemple le cas de Qwant, Searx ou de Startpage.

4. L'historique de navigation et les cookies

Par défaut, lors d'une navigation sur Internet, des données sont enregistrées dans l'ordinateur en fonction des recherches et connexions à des pages. Il s'agit notamment de l'historique des visites et des cookies. Si ces données peuvent faciliter les navigations futures, le risque est qu'elles soient consultées par des personnes indiscrètes (autres utilisat·rices du même ordinateur ou pirate malintentionné). Certaines d'entre elles (des "cookies tiers") permettent aussi à des acteurs du réseau de tracer les navigations d'individus. Heureusement, il est possible de limiter, contrôler ou supprimer ces enregistrements.

5. Les protections contre le traçage

Nos navigations sur Internet sont tracées par certains acteurs. Ce traçage permet d'établir des profils des consommateurs à destination des annonceurs, mais aussi de récupérer un grand nombre de données permettant des études statistiques très poussées. Ces pratiques sont très intrusives avec des dangers réels pour la vie privée aussi bien à titre individuel que collectif. Pour tenter de limiter ces risques, des modules de protection, tels qu'uBlock Origin ou Decentraleyes, sont disponibles.

6. Les mots de passe

Outil clé de l'identification sur les différents services en ligne, le mot de passe est souvent la seule barrière protectrice face à des intrusions non souhaitées aux conséquences potentiellement désastreuses. Il s'agit pourtant d'un outil trop souvent mal géré, de nombreu·ses utilisat·rices n'hésitant pas, par exemple, à employer des mots de passe très basiques, facilement cassables par un attaquant. Il est important de prendre conscience des enjeux des mots de passe et des méthodes permettant de les sécuriser facilement sans en complexifier la mémorisation pour se prémunir d'intrusion ou d'usurpation d'identité non souhaitées.

7-9. Les outils en ligne, hébergeurs de courriels et réseaux sociaux alternatifs

Une part conséquente de nos communications sociales est désormais réalisée en ligne : courriels, réseaux sociaux, outils de travail collaboratif ou de transmission d'informations... C'est un marché en développement rapide qui a attiré de nombreux acteurs. Les services proposés sont en apparence gratuits, mais ils ont en fait un cout indirect, car ils tracent une partie importante des activités des utilisat·rices et exploitent ensuite leurs données à des fins commerciales, sans grand respect pour la vie privée. Parfois ces données sont aussi récupérées par des services gouvernementaux à des fins de surveillance et de répression.

Afin de continuer à profiter des intérêts de ces services tout en se réappropriant ses données, le CECIL recommande différents outils, plus respectueux de la vie privée et des libertés, au travers de trois fiches :

- 7. Une consacrée aux dangers du *Cloud computing* et proposant des services bureautiques alternatifs en ligne,
- 8. Une consacrée à la réappropriation de ses courriels par le biais d'hébergeurs respectueux ou d'autohébergement,
- 9. Une dernière consacrée aux réseaux sociaux alternatifs à soutenir pour sortir de l'hégémonie des acteurs commerciaux majoritaires.

10. L'anonymat sur Internet

Il est facile de se sentir "anonyme" sur Internet, mais ce n'est bien souvent qu'une illusion. Un usage classique permet facilement d'identifier l'individu derrière des communications, adresse IP, contenu des communications, transmissions d'informations du navigateur et système d'exploitation, etc.
Pourtant, il existe de nombreuses raisons pour un individu de vouloir protéger la confidentialité de son identité. Pour ce faire, le CECIL présente des outils comme le réseau et le navigateur Tor et les réseaux privés virtuels (VPN).

11-12. Le chiffrement

Le stockage et la transmission d'une partie de plus en plus importante de nos existences par le biais informatique ont une conséquence dangereuse : il devient potentiellement facile pour une entité publique ou privée d'y accéder intégralement grâce à une faille informatique ou une opération de surveillance. Pour se prémunir en partie de ce risque, il existe des méthodes permettant de chiffrer ses données et ses communications pour éviter qu'une personne n'en prenne indument connaissance.

Au travers de deux fiches introductives, le CECIL recommande de recourir autant que possible au :

- 11. chiffrement des données,
- 12. chiffrement des communications.

13. Les ordiphones

Les ordiphones (ou smartphones) sont devenus des interfaces pour de nombreux usages du quotidien. Pourtant, ils constituent une faille importante pour la sécurisation des données et la protection des libertés. Ces petits ordinateurs sont plus difficilement contrôlables que leurs ainés, ils sont rarement « non connectés », les composants sont souvent plus spécifiques et les constructeurs exercent un pouvoir plus élevé sur ces matériels. Des méthodes simples permettent néanmoins de limiter les dégâts face à des atteintes possibles. Comme pour un ordinateur classique, il existe des applications et des bonnes pratiques permettant de mieux protéger ces appareils.

Pour continuer l'aventure...

Ces petites fiches constituent un premiers pa pour retrouver un peu d'intimité et de liberté dans le monde numérique. Il s'agit de reconquérir un certain contrôle sur ses données et une certaine autodétermination informationnelle.

Il ne s'agit toutefois que de préconisations générales qui peuvent ne pas correspondre à des cas particuliers. La sécurité est un processus, pas un produit, ces premiers pas permettent de se lancer dans ce processus. Pour aller plus loin et découvrir d'autres approches, le CECIL recommande de découvrir d'autres contenus et acteurs.

Fiche 01. Le système d'exploitation et le navigateur : deux outils fondamentaux

1.1 Le système d'exploitation : l'alternative des distributions Gnu-Linux

Lors de l'achat d'un ordinateur, l·a consommat·rice paye, souvent sans le savoir, un système d'exploitation. Il s'agit principalement de Mac OS X pour les ordinateurs d'Apple, et de Windows dans différentes versions pour les autres ordinateurs. Des pratiques similaires ont lieu avec les ordiphones (*smartphone*), qui comme le nom français l'indique sont en réalité bien plus des ordinateurs, capables aussi de téléphoner (voir la fiche 13). Si un système d'exploitation est nécessaire au bon fonctionnement d'une machine, rien n'oblige à recourir ou à acheter ces systèmes préinstallés. Il est possible, quoique moins commun, d'acheter un ordinateur sans ce cout supplémentaire, puis d'y installer un système de son choix compatible avec l'ordinateur.

Il existe notamment une alternative gratuite et plus respectueuse des libertés des utilisat·rices : les systèmes Gnu-Linux. S'appuyant sur le même noyau, de très nombreuses versions (on parle de distribution) coexistent. En plus d'être gratuites et libres, nombre d'entre elles sont d'une simplicité d'utilisation et d'installation comparable aux solutions par défaut évoquées précédemment. Il s'agit par exemple de Linux Mint, de Debian, de Fedora ou encore de Tails (The Amnesic Incognito Live System). La deuxième fiche précise l'intérêt pour ces systèmes d'exploitation d'être "libres", mais au-delà ces systèmes permettent de :

- économiser le prix d'une licence Windows,
- protéger des virus les plus communs (visant principalement Windows),
- donner un coup de jeune à un ordinateur un peu ancien… et cela sans perdre en fonctionnalités pour les usages standards (suite bureautique, édition photo, Internet).

Envie de sauter le pas ? Les sites des distributions précédemment citées expliquent de manière simple comment procéder (par exemple, le site doc.ubuntu-fr.org présente beaucoup d'informations et des tutoriels vidéo en français).(http://doc.ubuntu-fr.org/installation) Il en va de même pour Linux Mint. Si on redoute ces opérations qui, sans être trop complexes, demandent quand même quelques compétences, des bénévoles seront ravi·es d'aider lors d'évènements appelés "fêtes d'installation" (*install party*) ou, plus spécifiquement des "Ubuntu party". La plupart sont annoncées sur l'agenda du libre.

1.2 Le navigateur : un outil de base à choisir

Le passage de son ordinateur sous un nouveau système d'exploitation reste une opération qui nécessite une certaine forme d'implication et quelques efforts. À l'inverse, s'il est un outil clé sur lequel toute personne qui s'intéresse un peu à la protection de ses données personnelles et souhaite résister à l'emprise des monopoles ne devrait pas transiger, c'est bien son navigateur. Microsoft a profité de sa suprématie sur le marché des systèmes d'exploitation pour subrepticement incorporer à Windows d'autres logiciels clés : sa suite bureautique (Microsoft Office) et son navigateur (Edge ex Internet Explorer). Ce navigateur se retrouvait ainsi installé par défaut sur tous les ordinateurs dotés de Windows. La Commission européenne s'est saisie de ce cas et y a vu un abus de position dominante de Microsoft. Microsoft s'est alors vue contrainte de proposer aux utilisat·rices de Windows un choix entre Internet Explorer et plusieurs autres navigateurs concurrents, suggérés aléatoirement. Cette décision européenne a été inégalement respectée par Microsoft et trop de personnes n'ont pas été incitées à faire de choix. L'incitation à utiliser Google Chrome est elle aussi très forte, notamment sur ordiphone.

Il n'est jamais trop tard pour bien faire, et donc de choisir un autre navigateur que celui imposé "par défaut". Le CECIL recommande le navigateur Firefox dont l'efficacité n'a rien à envier à ses concurrents. En plus d'être très performant, son éditeur, la fondation Mozilla, est à but non lucratif et place certains engagements éthiques au cœur de sa stratégie : respect des standards du Web et de l'interopérabilité, liberté et ouverture du code source, combat pour la neutralité du net, respect de la vie privée de ses utilisat·rices…

D'autres éditeurs ont développé des modules complémentaires (dont uBlock Origin, Disconnect ou Privacy Badger qui eux aussi améliorent le respect de sa vie privée. Cela fait de Firefox un outil remarquable, adopté par environ un quart des internautes. En raison de ce succès et pour qu'il demeure gratuit, la fondation Mozilla a autrefois eu recours à un partenariat favorisant Google (proposé une fois encore "par défaut" comme moteur de recherche). Plus récemment, elle a accepté, sous la pression des industries culturelles, d'implémenter une fonctionnalité limitant les libertés (*Encrypted Media Extensions*). Malgré ces concessions regrettables, ce navigateur reste un très bon choix qui s'engage dans la protection des libertés et de la vie privée.

Les plus engagé·es préfèreront peut-être d'autres navigateurs libres et sans concessions, tels que Palemoon, Midori. Il est également possible d'utiliser le navigateur TOR qui s'appuie sur Firefox en ajoutant des fonctionnalités de protection des communications ou même Chromium la base libre de "Chrome" sans le traçage de Google. Vous pestez contre la surveillance de masse et utilisez encore Edge ou Chrome ! Il est temps de changer de navigateur et si possible d'aller un peu plus loin.

Pour aller plus loin :

Les sites des principales distributions Gnu-Linux citées : Ubuntu.com, LinuxMint.com, Debian.org, GetFedora.org, Tails (The Amnesic Incognito Live System). Les sites des navigateurs cités : Firefox.com, Palemoon.org, Midori-Browser.org.
Notons qu'il est tout à fait possible d'installer, sans réelles difficultés, une distribution Gnu-Linux sur les ordinateurs Apple *à priori* depuis les ordinateurs postérieurs à 2006.

La vente d'un ordinateur où est déjà installé un système d'exploitation payant est susceptible de constituer une pratique de vente liée déloyale. La jurisprudence est fluctuante, mais des associations telles que l'AFUL et l'UFC Que Choisir sont parvenues à obtenir des décisions contraignant le vendeur à rembourser le système d'exploitation jugé non nécessaire par l'utilisat·rice. Sur ce sujet :

- la synthèse du combat de l'AFUL : *Racketiciel : Dernier "tir judiciaire"*,
- la page wiki consacrée à "la vente liée en matière de logiciels" sur la grande bibliothèque du droit,
- malheureusement, la jurisprudence européenne est favorable à cette pratique, voir cet article de NextInpact, "Pourquoi la justice européenne a sanctuarisé la vente liée PC et OS".

Fiche 02. Les logiciels libres

Les systèmes d'exploitation Gnu-Linux comme les navigateurs Firefox ou Midori présentés Fiche 1 sont tous des "logiciels libres". Ce choix est loin d'être anodin. Ces logiciels libres participent à garantir le contrôle des utilisat·rices sur leurs logiciels, leurs données et, par conséquent, leurs libertés. Ils sont un socle minimal pour que l'informatisation de la société puisse se faire dans le respect des personnes. Le CECIL apporte son soutien à l'utilisation et au développement de logiciels libres, pierre angulaire du respect de nos libertés.

2.1 Présentation générale

Un logiciel ou programme est une suite d'instructions destinées à être exécutées par un ordinateur. Depuis le milieu des années 90, les logiciels peuvent être protégés par des droits de propriétés intellectuelles et le sont majoritairement. Ainsi, la majorité des éditeurs de logiciels proposent-ils essentiellement des licences d'utilisation commerciales en échange d'une rémunération directe (un prix) ou indirecte (publicité, part de marché…). Surtout, ils conservent et protègent jalousement le code source de leurs logiciels. Ces instructions lisibles par l'humain sont traduites en langage binaire, qui lui est illisible par l'humain, mais est exécutable par la machine. C'est ce seul programme en binaire qui est transmis par les éditeurs propriétaires. Ce processus rend impossible, aussi bien pour une personne lambda que pour un·e développeu·se aguerri·e, d'accéder au fonctionnement exact du logiciel, ses fonctionnalités et encore moins de le modifier. Sans accès au code source, l'utilisat·rice doit donc faire aveuglément confiance à l'éditeur, qui seul peut analyser et vérifier le logiciel et a le pouvoir d'implémenter des fonctionnalités cachées qui serviraient ses propres intérêts ou ceux d'un programme de surveillance. À l'inverse, un logiciel mis sous licence "libre" s'engage à respecter 4 grandes libertés définies par la Free Software Foundation :

- Liberté 0, d'exécuter le programme, pour tous les usages.
- Liberté 1, d'étudier le fonctionnement du programme, et de l'adapter à ses besoins. Pour ceci l'accès au code source est une condition nécessaire.
- Liberté 2, de redistribuer des copies, donc d'aider son voisin.
- Liberté 3, d'améliorer le programme et de publier des améliorations, pour en faire profiter toute la communauté. Pour ceci l'accès au code source est une condition nécessaire.

Lorsque l'on qualifie un logiciel "libre", on fait ainsi référence aux libertés de ses utilisat·rices, et non pas au prix. Il reste fondamental de bien comprendre que "logiciel libre" ne signifie pas "non commercial"; on trouve des logiciels libres gratuits, mais d'autres sont payants à cause d'un service supplémentaire fourni. Cette ambigüité est plus prononcée en anglais ou le terme "*free*" a les deux significations. Cette liberté de maitriser le logiciel s'apparente à la notion de "liberté d'expression". Même sans intention de modifier ces logiciels libres, les utiliser permet de les soutenir et contribuer à leur diffusion et popularité en incitant d'autres à les améliorer. De plus, on peut diffuser le logiciel sans être coupable de contrefaçon. Ces logiciels sont de qualité et d'efficacité équivalente, parfois même supérieure, aux solutions propriétaires. Pour qu'un logiciel soit considéré comme libre, il doit être placé sous une licence garantissant les 4 libertés telles que la licence GNU-GPL, la licence française CECILL (pour CEa Cnrs Inria Logiciel Libre) ou la licence permissive MIT. C'est par exemple le cas de Firefox pour le navigateur Web, mais aussi de LibreOffice qui sert de parfait remplacement libre et gratuit à Microsoft Office (sur Windows, OS X et Gnu-Linux). On peut également citer Thunderbird comme outil de gestion des courriels, VLC pour la lecture de contenus multimédias, ou GIMP pour l'édition d'image.

2.2 Les avantages des logiciels libres :

- **Le recyclage de fonctionnalités :** les développeu·ses de logiciels libres peuvent s'appuyer sur du code fiable déjà développé et ainsi éviter de devoir tout reprendre à zéro. En empruntant des portions de code source à d'autres logiciels, ils gagnent du temps qui peut être consacré au développement de nouvelles fonctionnalités.
- **L'efficacité et la fiabilité :** le code étant mis à disposition de tous sur des "plateformes de développement" (type Github exemple Framagit, chacun peut participer selon ses compétences au développement du logiciel. Cela permet d'explorer des solutions techniques originales et adaptées à des besoins locaux. De plus, dès qu'un bogue ou une faille dans le code est détecté, des spécialistes peuvent intervenir rapidement pour proposer des correctifs et sécuriser le logiciel.
- **Le respect des standards :** les sociétés commerciales abusent de normes qui leurs sont propres rendant impossible ou complexe la communication entre logiciels. À l'inverse, les logiciels libres garantissent l'interopérabilité entre logiciels en respectant les normes ou standards. C'est un engagement fort de la communauté du libre.
- **Une garantie pour la sécurité et les libertés :** l'accès au code source permet que ces logiciels soient audités et de vérifier qu'il n'y a pas de dissimulation de fonctionnalités cachées ou de portes dérobées (*backdoor*). Même pour l'individu inexpert, cette transparence est une garantie en soi.
- **L'indépendance et la pérennité :** les logiciels propriétaires sont tributaires de leurs éditeurs et si une entreprise qui développe un logiciel fait faillite, abandonne ou limite son développement, les travaux et modules dépendants de celui-ci peuvent devenir inutilisables ou obsolètes. Avec un logiciel libre, quiconque peut redémarrer un projet qui aurait été mis de côté et faire revivre le logiciel. Les logiciels libres sont donc une garantie de pérennité. De la même façon, si un éditeur décide d'introduire des fonctionnalités contestables ou d'abandonner le projet, une autre équipe de développement peut décider de repartir du code source précédent et de recréer un clone sans celles-ci (voir l'exemple d'OpenOffice dont le code a été repris, notamment, par LibreOffice). Cela offre une indépendance vis-à-vis de cet éditeur.
- **Un avantage économique :** avoir recours à des logiciels libres évite d'acheter ou de renouveler des licences d'utilisation. De plus en plus d'administrations et d'associations font ce choix et consacrent ces économies à des services supplémentaires. Le logiciel libre a donc de grands avantages, il implique toutefois certains ajustements en raison de la diversité de ses pratiques.

2.3 Les inconvénients des logiciels libres :

- **Une offre dispersée :** la multiplication de logiciels proches, basés sur du code similaire, est une garantie de diversité, mais peut diluer les efforts des développeu·ses. Des emprunts aux différents projets sont possibles, mais la coordination mondiale reste difficile. De la même façon, cette dispersion peut constituer un frein à la diffusion vers les utilisat·rices par une surabondance de choix de logiciels presque équivalents. Fort heureusement, la plupart des plateformes de diffusion de logiciel libre offrent un classement et une sélection c'est le cas de l'association Framasoft).
- **Des modèles économiques complexes :** il est plus difficile d'obtenir une rémunération avec des logiciels libres qu'avec des logiciels propriétaires. La seule diffusion de logiciels libres n'étant pas payante, le modèle économique doit être pensé en amont pour amortir les couts de développements en offrant, par exemple, un service efficace rémunéré. L'engagement communautaire permet de compenser en grande partie cet inconvénient, mais il reste parfois difficile d'obtenir un financement stable et durable pour des développeu·ses libres indépendant·es.

2.4 Une implication nécessaire de tous

Les logiciels libres sont mis à la disposition de tous. Pour que ce modèle fonctionne bien, il requiert un minimum de solidarité. Ainsi, tout développeur peut participer à l'amélioration du logiciel. De son côté, l'utilisat·rice profane a la possibilité de participer en signalant les bogues (*bug*), en proposant des améliorations possibles, en réalisant des traductions de la documentation ou en diffusant le logiciel. L'implication solidaire des utilisat·rices peut aussi se traduire sous forme de dons pour participer aux développements de logiciels qui

bénéficieront à tous. Les développeu·ses et les utilisat·rices profanes et actifs, forment "la communauté" nécessaire à l'essor du logiciel correspondant. L'April, Framasoft, la Free Software Fondation Europe et l'Aful sont les quatre principales associations de promotion du logiciel libre en France. Il en existe bien d'autres, dont beaucoup de locales. Il ne faut pas hésiter à se renseigner ou à les rejoindre ! On notera également qu'il existe de nombreux évènements liés à l'informatique libre. Des "fêtes d'installation" (*install parties*) visant à aider les particuliers à faire le grand saut et à installer une distribution Gnu-Linux sur leur ordinateur, mais également des évènements de grande importance comme l'Open World Summit, qui se réunit annuellement à Paris, le Capitole du Libre ou les Rencontres Mondiales du Logiciel Libre.

Pour aller plus loin :

En plus des sites des différentes organisations citées dans cette fiche : (la Free Software Foundation, l'April, Framasoft, la Free Software Fondation Europe, l'Aful, l'Open Source Initiative qui regorgent d'informations complémentaires sur le mouvement du libre, il est possible de consulter :

- le livre blanc de l'April sur les modèles économiques du logiciel libre,
- les travaux de l'INRIA en matière de logiciel libre, notamment dans le cadre de l'IRILL, dont deux guides analysant différentes licences libres,
- le logiciel libre bénéficie d'un soutien et d'une reconnaissance importante de la part de l'UNESCO, où un portail dédié est mis à disposition (la version à jour est en anglais).

Fiche 03. Les moteurs de recherche alternatifs

Outil central de nos pratiques sur Internet, un moteur de recherche permet de lancer une recherche sur un sujet, une personne, une organisation... à l'aide de différents critères et mots-clés afin d'identifier des contenus disponibles et pertinents. Cette façon de rechercher aisément des documents permet de vérifier rapidement l'existence, la notoriété et les sources d'une information. En 2015, plus d'une centaine de moteurs de recherche sont disponibles : le trop célèbre Google, mais aussi Bing, Yahoo, le moteur russe Yandex ou le chinois Baidu, etc. Même si la plupart de ces outils ont une "politique de confidentialité", les intérêts commerciaux de leurs éditeurs restent prioritaires face aux droits des individus. Ainsi, chaque recherche lancée s'accompagne d'une collecte discrète de données concernant les préférences de l'utilisat·rice ainsi que des données relatives à l'ordinateur utilisé. Par ce biais, les moteurs de recherche accumulent une quantité inimaginable de données sur les individus et la société dans son ensemble. Ces informations sont monnayables, voire utilisables, pour du contrôle social. Le quasi-monopole du moteur de recherche de Google en Europe (90 % de parts de marché) lui donne donc un pouvoir redoutable. À côté de ces moteurs, d'autres sont moins connus et sont une alternative intéressante pour la protection de ses données tels que DuckDuckGo, Startpage ou Qwant. Il s'agit ici de les mettre en valeur pour inciter les personnes soucieuses de préserver leur vie privée à changer leurs pratiques.

3.1 Qwant : un projet français en développement

Si, à son lancement en 2013, le projet était peu convaincant, le moteur de recherche Qwant a bien compris l'enjeu des révélations d'E. Snowden et se présente désormais comme une alternative valable pour protéger sa vie privée et ne semble pas cesser de s'améliorer.

Des mots de l'équipe : "*La philosophie de Qwant repose sur 2 principes : ne pas tracer les utilisat·rices et ne pas filtrer le contenu d'Internet. Nous faisons tout notre possible pour respecter la vie privée des internautes tout en garantissant un environnement sécurisé et des résultats pertinents.*" et "Nous ne cherchons jamais à savoir qui vous êtes ou ce que vous faites".

Il s'agit donc d'une alternative efficace pour protéger sa vie privée. La société Qwant a le mérite d'être située en France, d'avoir une politique de protection des données très poussée et de prendre publiquement position pour le respect de la vie privée. En plus de cela, le moteur propose une approche différente de celle de Google pour ses résultats. Les résultats de pages Web sont complétés automatiquement par des résultats issus d'articles de la presse en ligne, de Wikipédia, de Twitter et d'images permettant potentiellement d'accéder plus rapidement à l'information ou au contenu désiré. Il est facilement possible de ne voir qu'une catégorie de résultats. Une version "lite" plus épurée existe également.

S'il utilise encore les données provenant d'autres moteurs de recherche, Qwant développe son propre moteur et donc sa propre indexation du Web afin de limiter sa dépendance face aux autres et ses engagements en termes de protection de la vie privée se multiplient.

Son financement repose sur de l'affichage publicitaire non traçant, lié uniquement à la requête, ainsi que sur de l'affiliation *via* les achats réalisés sur son interface de "Shopping" ou les liens publicitaires sans causer donc de réels soucis relatifs à la vie privée.

Pour le passer en moteur par défaut sur Firefox, rien de plus simple :

> Une fois sur la page d'accueil du moteur, cliquer sur l'icône en forme de loupe de la barre de recherche de Firefox et cliquer sur "Ajouter "Qwant". Il faudra ensuite recliquer sur la loupe, cliquer sur "Modifier les paramètres de recherche". Dans l'interface ouverte, choisir "Qwant" comme moteur par défaut.

Les avantages d'utilisation de Qwant :

- **Confidentialité :** l'adresse IP est dissociée de la recherche et n'est pas conservée, il n'y a pas de dépôt de cookie ni d'utilisation d'aucun dispositif de traçage, il n'y a pas de récupération d'informations personnelles à l'insu de l'utilisateur et aucune communication à des sociétés privées.
- **Neutralité :** il propose les mêmes résultats d'un utilisateur à l'autre, sans donc tenir compte d'un "profil" ou de ses précédentes recherches, qu'il ne conserve pas. Ainsi, on évite la personnalisation des contenus, qui introduit un biais de confirmation, et on obtient un résultat plus objectif.
- **Sécurité :** la connexion est sécurisée en utilisant le protocole de communication chiffrée (HTTPs).
- **Localisation :** Qwant est une société située en France et financée par des investissements européens, ses résultats sont très satisfaisants pour les requêtes en français.
- **Fonctionnalité :** Qwant offre une nouvelle approche intéressante des recherches en enrichissant les résultats généraux d'informations de Wikipédia ainsi que de sources de presse et de réseaux sociaux. Qwant offre aussi la fonctionnalité des "!bang" conceptualisée par DuckDuckGo
- **Engagements publics :** une partie des revenus de Qwant sont de plus consacrés à des projets liés à l'amélioration de la sécurité et de la vie privée et la société s'engage publiquement sur les questions de vie privée et de neutralité.

Quelques nuances :

Si la localisation française est un atout d'un point de vue fiscal et en termes de respect du droit européen sur la protection des données, cela soumet aussi la société à la législation française. Même sans surveillance, Qwant fonctionne malgré tout via un modèle publicitaire soutenu par du capital-investissement.

3.2 DuckDuckGo : un moteur de recherche qui respecte la vie privée

Lancé en 2008, un des slogans de DuckDuckGo est : Google vous traque, pas nous. Ce moteur aspire à limiter autant que possible la récupération et la conservation des données de ses utilisat·rices. Le site n'enregistre pas les requêtes et affiche une opposition ferme au traçage. Il s'agit d'un métamoteur de recherche : il utilise son algorithme pour classer les résultats issus d'autres sources d'informations ouvertes et enrichit les réponses. Ainsi, au-delà même du plus grand respect de la vie privée et des engagements du moteur, ses fonctionnalités propres en font une alternative intéressante à Google. Pour le passer en moteur par défaut sur Firefox, rien de plus simple :

> Une fois sur la page d'accueil du moteur, cliquer sur l'icône en forme de loupe de la barre de recherche de Firefox et cliquer sur "Ajouter "DuckDuckGo"". Il faudra ensuite recliquer sur la loupe, cliquer sur "Modifier les paramètres de recherche". Dans l'interface ouverte, choisir "DuckDuckGo" comme moteur par défaut.

Les avantages d'utilisation de DuckDuckGo :

- **Confidentialité :** il ne stocke pas d'informations personnelles concernant les utilisat·rices, pas même leurs adresses IP (adresse d'identification des ordinateurs sur Internet). Il offre de nombreuses garanties contre le traçage et conserve le minimum de données possibles et aucune directement identifiante.
- **Multilingue :** l'interface existe en français et l'essentiel des pages et des fonctionnalités sont désormais également traduites.
- **Neutralité :** comme Qwant il propose les mêmes résultats d'une personne à l'autre.
- **Sécurité :** il favorise l'utilisation de sites sécurisés (HTTPs - accès sécurisé au site Internet) et est disponible via le réseau TOR.
- **Fonctionnalité :** DuckDuckGo propose un certain nombre de fonctionnalités spécifiques. En plus de donner des résultats "directs", tels que des extraits de fiches Wikipedia ou des cartes OpenStreetMap, il peut faire des recherches spécifiques (date, lieu…) et même rechercher sur un autre moteur *via* DuckDuckGo. Par exemple, en indiquant *"!t la requête"*, on est automatiquement redirigé vers le thesaurus. Ainsi il est possible d'avoir les résultats de Google via Startpage (*"!sp la requête" ou dans le pire des cas... !g "la requête"*).
- **Engagements publics :** une partie des revenus de DuckDuckGo sont de plus consacrés à des projets de développement de logiciels libres protecteurs de la vie privée.

Quelques nuances :

Le siège social de DuckDuckGo est situé aux États-Unis (en Pennsylvanie). L'entreprise est donc soumise à la loi américaine et potentiellement à des injonctions judiciaires ou administratives d'enregistrement et de transmission de données. Le moteur se défend toutefois de cette possibilité et indique qu'il ne s'y soumettrait pas. On pourrait également lui reprocher ses partenariats publicitaires avec Amazon et eBay, qui sont loin d'être des défenseurs de la vie privée. Il faut toutefois rappeler que les sources de financement sont rares, que les publicités sont minimales, qu'elles sont désactivables dans les paramètres et qu'il est loin d'être le seul acteur à y avoir recours (c'est aussi le cas du système d'exploitation libre Ubuntu).

3.3 Startpage : Google sans le traçage

Depuis 2006, le moteur de recherche Startpage prône comme politique le respect intégral de la vie privée de l'internaute et de ses informations personnelles. Contrairement à DuckDuckGo installé aux États-Unis, donc soumis à la législation américaine (Patriot Act…), Startpage est basé aux Pays-Bas. Il est donc soumis à la législation européenne et travaille avec la CNIL néerlandaise. Il ne s'agit pas d'un moteur de recherche, c'est-à-dire qu'il ne dispose pas de son propre algorithme d'indexation et de recherche, mais fournit les résultats de Google. Dans leurs mots "Ainsi, vous obtenez les résultats Internet du moteur de recherche le plus renommé avec la protection de la confidentialité du moteur de recherche le plus privé au monde".

Les avantages d'utilisation de Startpage :

Toutes les adresses IP et les autres données de recherche archivées sont effacées sous 48 h, il n'y a pas d'enregistrement de cookies identifiants dans l'ordinateur, il n'y a pas de récupération d'informations personnelles à l'insu de l'utilisateur, donc aucune communication à des sociétés privées, localisation de la société en Europe, aux Pays-Bas. Les résultats sont équivalents à ceux de Google.
Les grands atouts de DuckDuckGo ou de Qwant sont présents : absence de traçage, cookies limités aux stricts besoins de la recherche, absence de personnalisation des résultats, HTTPs…

Des limites :

La société Surfboard Holding, éditrice de Startpage est dépendante de Google pour ses résultats de recherche et se finance par le biais du programme publicitaire de Google : Adsense, ce qui implique certaines formes de

traçage indirect. Sans pouvoir associer l'adresse IP à la recherche, Google aura quand même connaissance de caractéristiques techniques de la recherche (mots-clés, heure, indication linguistique, affichage de la publicité, etc.) et pourra reprendre le traçage si l'internaute clique sur un lien publicitaire.

Sans être parfaits, Qwant, DuckDuckGo et Startpage constituent toutefois des alternatives à privilégier au monopole de Google et à sa propension à vendre notre vie privée. D'autres petits moteurs fiables et protecteurs existent, Blekko.com, Searx.me, ou encore Yacy.net.

3.4 Yacy : un projet à soutenir

Yacy est particulièrement intéressant d'un point de vue du respect de l'utilisateur. Il est sous licence libre, ne stocke pas de données à caractère personnel, a un fonctionnement décentralisé, ne comporte pas de publicité, etc. Il est toutefois différent des autres moteurs en ce qu'il requiert l'installation d'un logiciel sur sa propre machine. Fonctionnant sur un modèle "de pair à pair" pour l'indexation des pages, il n'y a pas de serveur central. C'est un avantage, mais cela implique une coopération active de personnes prêtes à jouer le rôle de pair/serveur décentralisé. Sans être totalement prêt à remplacer un moteur de recherche classique pour des usages habituels, il s'agit vraiment d'un projet à découvrir et à soutenir.

3.5 Les moteurs de recherche interne à des sites

De nombreux sites disposent de leur propre moteur de recherche interne. Certains de ces moteurs spécifiques peuvent être utilisés directement en les installant dans la barre de recherche de Firefox. Ainsi, si on cherche fréquemment un article de Wikipédia, une définition précise sur le Portail lexical du CNRS ou une aide à la traduction sur Linguee.fr, nul besoin de l'intermédiation d'un moteur généraliste, que ce soit Google ou DuckDuckGo. On peut ajouter ces moteurs à sa barre de recherche. Sur Firefox, il suffit dans la majorité des cas de :

> Aller sur la page d'accueil du site, cliquer sur la loupe de la barre de recherche de la barre d'outils de Firefox et cliquer sur « Ajouter le moteur » et il sera mémorisé.

Ensuite, on peut cliquer sur la loupe quand on s'apprête à faire une recherche puis cliquer sur l'icône du moteur voulu pour cette seule recherche. Il est aussi possible de regarder si le moteur est référencé dans la base de Mozilla et l'ajouter par ce biais.

Pour aller plus loin :

Pour un état des lieux de la question, voir la fiche Wikipédia « Moteurs de recherche » listant les moteurs de recherche protecteurs de la vie privée.

Des articles et compléments sur Qwant :
* J. Lausson, Numerama.com, *Eric Léandri (Qwant) : les internautes « doivent-ils désormais se méfier de l'État ? »*,
* Korben.info, *Qwant – Mon retour après 1 mois de test*,
* D. Cuny, Rue89, *Qwant, le « Google français » ? On ne ricane pas, s'il vous plait*.

Des articles et compléments sur DuckDuckGo :
* Netpublic.fr, *Apprendre à utiliser DuckDuckGo, moteur de recherche qui respecte la vie privée : 6 tutoriels*,
* le site de DuckDuckGo, Donttrack.us. Le métamoteur Searx est notamment mis à disposition par Framasoft sur Framabee.org.

Fiche 04. L'historique de navigation et les cookies

4.1 Présentation

Edge, Google Chrome, Mozilla Firefox (évoqués dans la fiche 1) stockent un grand nombre d'informations durant les navigations. Il s'agit de traces concernant les recherches et les pages des sites visitées.

Ces traces comportent :

- un historique des navigations avec des éléments d'identification des pages (adresse HTTP, date de visite…),
- une mémorisation des éléments indiqués par l'utilisat·rice (données de formulaire, données d'identification à des sites Internets et mots de passe…),
- des données conservées visant à faciliter les navigations ultérieures (cache, préférences de sites, cookies).

L'ensemble de ces informations est appelé "l'historique de navigation". Celui-ci permet à l'internaute de retrouver facilement les sites visités et de ne pas avoir à refournir toujours les mêmes informations. La mémorisation de ces saisies s'effectue par défaut et souvent de façon automatique. Toutes ces informations sont conservées sur l'ordinateur de l'utilisat·rice.
Parmi ces informations sont stockés des petits fichiers textes appelés "cookies". Ces suites d'informations sont créées et enregistrées à la demande du site visité. Ces cookies peuvent apporter des facilités pour se connecter ultérieurement, pour conserver des paramètres ou pour utiliser un site en général. Ils sont souvent nécessaires pour réaliser des achats en ligne. Il ne s'agit pas de fichiers exécutables et ce ne sont pas des virus, mais étant interrogeables, ils offrent des possibilités de traçage des activités de l'internaute. Par exemple, même sans être "cliqués", les boutons de partage des réseaux sociaux, présents sur de nombreuses pages, permettent à Facebook, Google et Twitter de tracer les visites. Pour se préserver de cette intrusion : voir la fiche 5

4.2 Limiter les traces locales de ses communications sur Internet

Afin de réduire ces traces, les principaux navigateurs Internet proposent des outils de navigation "privée". La navigation privée permet, théoriquement, d'utiliser Internet en minimisant les traces sur son propre ordinateur : lorsque l'outil est activé, il n'y a pas d'enregistrement d'historique de navigation, de données de formulaires, des téléchargements effectués, ni de conservation de cookies. Les données sont utilisées dans l'immédiat, mais sont supprimées dès la fin de l'opération ou de l'activité de l'internaute.

> À titre d'exemple, il est possible de lancer une fenêtre de navigation privée sur Firefox en appuyant sur : "Ctrl + Maj + P" (ou Pomme + Maj + P sur Mac) ou en cliquant "Nouvelle fenêtre de navigation privée" dans les options.

Il faut d'ailleurs noter que depuis quelque temps, la navigation privée de Firefox offre aussi une protection contre le traçage (voir fiche 5) !

Il est aussi possible de demander à Firefox de ne jamais conserver d'informations :

> dans l'onglet "Vie privée" des "Options" (ou "Préférences"), choisir le paramètre "ne jamais conserver l'historique".

Sans utiliser la navigation privée, on peut également supprimer tout ou partie de l'historique de navigation régulièrement.

> toujours dans l'onglet "Vie privée", cliquer sur "Effacer votre historique récent", ou, à partir du Menu, onglet "Historique", puis "Supprimer l'historique récent". Choisir les éléments que l'on souhaite supprimer ou conserver et définir la période de suppression.

On peut ainsi supprimer toutes les traces temporaires et ne conserver que les favoris et autres mots de passe enregistrés. L'utilisation de la navigation privée ou la suppression manuelle de l'historique sont des fonctions importantes en particulier si l'ordinateur est partagé. C'est par exemple le cas pour l'utilisation d'un ordinateur public. Il s'agit là de protéger sa vie privée face aux personnes ayant accès au même ordinateur qui peuvent être des proches ou non.

4.3 Les limites de la gestion locale de ses traces

L'utilisation de la navigation privée ne protègera toutefois pas de nombreuses possibilités de surveillance des communications ou des données de connexion par :

- des sites Web consultés,
- des employeurs ou gestionnaires locaux de l'accès réseau (selon les paramétrages choisis),
- les Fournisseurs d'Accès Internet,
- des mouchards malveillants, virus ou intrusions sur la machine,
- d'une interception en direct de la communication.

Même s'il s'agit d'une protection limitée, il est important de connaitre et maitriser la gestion de ses propres traces. Cela permettra d'éviter que des proches ou un tiers indésirable ne prennent facilement connaissance d'informations jugées personnelles. Cela n'empêchera toutefois pas d'être tracé et profilé par de grandes entreprises en ligne, ni de limiter les possibilités de surveillance des États. D'autres solutions doivent être mises en œuvre, qui elles aussi ont leurs limites. Pour cela, direction les autres fiches !

Pour aller plus loin :

La CNIL dispose d'une documentation assez complète sur les enjeux des cookies au regard de la vie privée. Ces informations sont regroupées dans un dossier sur les cookies et autres traceurs.
Elle dispense ainsi des conseils côté utilisateur, mais aussi sur les obligations des responsables de site à cet égard. Elle a également mis au point un outil, Cookieviz, malheureusement uniquement disponible sur Windows, qui permet de visualiser la création et le fonctionnement des cookies sur votre ordinateur (il existe une vidéo de présentation).

Fiche 05. Les protections contre le traçage

Internet a de nombreux avantages, mais n'est pas sans défauts. La principale méthode de financement des sites Internet est la publicité. L'adage est connu "si c'est gratuit, vous êtes le produit". De nombreux sites vendent donc le "temps de cerveau disponible" de leurs utilisat·rices reportant les couts sur l'achat des produits ou services de l'annonceur. Au-delà du débat sur le bienfondé de la publicité, celle-ci conduit souvent sur Internet au traçage de données personnelles. Ce traçage peut aller jusqu'au profilage détaillé des utilisat·rices, qui peut s'avérer extrêmement dangereux en termes de surveillance. En effet, pour optimiser les annonces, les sites collectent de nombreuses données qui servent autant :

- dans une approche générale, à identifier les profils des consommateurs potentiels,
- dans une approche individualisée, à proposer les publicités les plus susceptibles de conduire à l'acte d'achat.

C'est la principale source de revenus des deux géants Google et Facebook qui tirent la quasi-totalité de leurs revenus de la publicité et de l'exploitation des données personnelles. Ils représentent à eux deux autour de 50 % du marché publicitaire en ligne et ne cessent de croitre.

Les individus sont ciblés par ce biais en tant que consommateurs, parfois dans des proportions qu'ils n'imaginent pas. Leurs données peuvent également être exploitées à des fins de gestion ou de surveillance des populations. Les révélations Snowden ont montré que c'était le cas avec certains grands acteurs du numérique, notamment ceux souvent appelés les "GAFAM" (Google Amazon Facebook Apple et Microsoft).

Le problème est toutefois plus général notamment en raison des "courtiers en données" (*databrokers*) qui même s'ils sont moins connus accumulent et exploitent des quantités colossales de données personnelles. Certains de ces acteurs ne se contentent pas d'utiliser ces données pour des motifs commerciaux, mais n'hésitent pas à les utiliser dans des cadres politiques tels que des élections.

Cette surveillance en ligne est donc extrêmement problématique d'un point de vue économique comme démocratique.

Il existe pourtant une option présente dans les navigateurs qui vise à signifier aux sites visités que l'on ne souhaite pas être tracé, le "*Do Not Track*" (ne pas tracer). Sur Firefox :

> dans l'onglet "Vie privée" des options, cocher "Indiquer aux sites que je ne souhaite pas être pisté".

Malheureusement, il s'agit d'un projet de standard qui n'a pas abouti et la plupart des sites visités ne respectent pas ce souhait et au contraire cela peut leurs permettre de constituer des bases d'"internautes qui

ne veulent pas être tracés". Le CECIL propose donc d'utiliser des outils plus protecteurs pour résister autant que possible à ces pratiques de traçage.

Il faut relever que Firefox protège, par défaut, contre certaines opérations de traçage, notamment en navigation privée et continue d'avancer en ce sens.

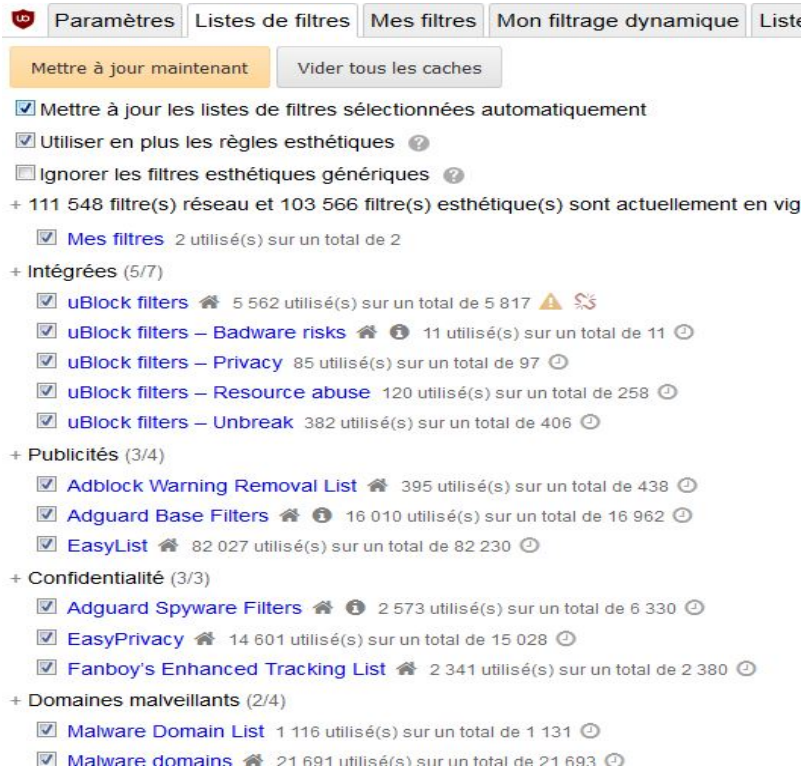
Pour compléter cette protection et l'améliorer, il est pertinent d'installer des modules qui vont bloquer au maximum les tentatives des sites pour obtenir des données sur l'utilisat·rice et l·a suivre dans ses navigations sur le Web.

5.1 uBlock Origin la star des "Adblock", contre le traçage publicitaire

Le plus célèbre d'entre eux est "Adblock Plus" qui fait disparaitre des navigations la majorité des encarts publicitaires. Toutefois en raison de ses nouvelles pratiques commerciales critiquables, le CECIL conseille plutôt d'installer uBlock Origin. Celui-ci ne comporte pas les fonctionnalités critiquées et est bien plus efficace et moins gourmand en mémoire.
Pour l'installer facilement sur Firefox, il suffit de l'ajouter *via* la plateforme d'extension de Firefox.

Il s'installe, par défaut, avec notamment une liste de base de publicités bloquées (*Liste-FR+EasyList*) qui va stopper la plupart des publicités sur Internet ainsi que la liste "EasyPrivacy" antitraçage. Ces listes sont tenues à jour automatiquement et peuvent aussi être complétées. La sélection par défaut est efficace, mais pour en ajouter :

Aller dans les préférences du module (Options – Modules – Préférences uBlock Origin), onglet "Listes de filtres" et activer les listes pertinentes (par exemple celles classées en "Confidentialité" et en "Réseaux sociaux").



Les listes "Fanboy's Anti-Thirdparty Social" et "Fanboy's Social Blocking List" sont importantes, car elles bloquent les cookies dits "tiers" tels que ceux de Facebook, Google et Twitter, présents sur de nombreuses pages cachés derrière les boutons de "partage" (G+1, Like, Tw). Ceux-ci permettent à ces sociétés de connaitre les sites visités.

Il est aussi possible d'ajouter des blocages personnalisés. Par exemple, pour les utilisat·rices de Facebook, pour bloquer la fonctionnalité permettant aux participants à une discussion de voir si des messages ont été "vus", il faut aller dans l'onglet "Mes filtres" et ajouter :

> ||facebook.com/ajax/mercury/change_read_status.php$xmlhttprequest

5.2 Disconnect.me, en complément

Bien qu'uBlock Origin puisse bloquer les dispositifs de traçage, il n'est pas totalement destiné à cela et Disconnect.me reste un bon complément. Même si uBlock et Disconnect se recoupent partiellement, leurs listes de filtres ne sont pas identiques. Ainsi, Disconnect.me limite aussi les traçages d'analyse des consultations, ou des réseaux sociaux…

> Pour ajouter Disconnect.me à Firefox, aller sur la page de l'extension dans la base de Mozilla, puis "Ajouter à Firefox".

Pour compléter l'installation :

> Cliquer sur l'icône "D" de Disconnect.me et cliquer sur celle à côté de "Content" pour bloquer aussi les traqueurs contenus dans les articles (attention cela peut rendre certains contenus inaccessibles, il suffira de le décliquer pour ces contenus spécifiques).

Ces deux extensions protègeront contre un grand nombre de traqueurs.

5.3 Decentraleyes

De nombreux sites Internet font appel, par praticité à des ressources basiques stockées chez des sites tiers appelé des "*Content Delivery Network*" (CDN). Certains de ces CDN en profitent pour tracer les visiteurs de ces sites Internet. Decentraleyes va installer ces ressources basiques sur l'ordinateur et renvoyer les requêtes en local au lieu de permettre aux CDN de récupérer des données. C'est donc un complément intéressant pour limiter le traçage en ligne.

> Pour ajouter Decentraleyes à Firefox, aller sur la page de l'extension dans la base de Mozilla, puis "Ajouter à Firefox".

5.4 Privacy Badger, une protection dynamique de l'EFF

Privacy Badger, de l'Electronic Frontier Foundation, a pour objectif de combiner les avantages des différentes extensions protectrices de la vie privée (dont uBlock et Disconnect) au sein d'une seule extension. Il s'agit toutefois d'un projet récent et qui se consacre pour le moment principalement aux cookies traceurs. Il n'a pas pour vocation de bloquer les publicités qui ne tracent pas leurs utilisat·rices. Son fonctionnement est automatique et dynamique (il examine les actions d'une page pour savoir quoi bloquer), il n'est pas toujours évident de comprendre son impact, mais il peut constituer un module intéressant pour se protéger.

Ces modules sont une protection non négligeable, mais pour s'assurer qu'aucune requête ne sera suivie à travers le Web, d'autres précautions sont nécessaires.

5.5 Quelques autres extensions intéressantes

- En naviguant sur Internet, on transmet par défaut les caractéristiques du navigateur et du système d'exploitation. Pour le constater, on peut réaliser ou tester le "Panopticlick" de l'EFF. Pour éviter d'être trop transparent et choisir les informations transmises, on peut utiliser User Agent Switcher. Ce module permet de faire croire que la requête provient, par exemple, d'une vieille version d'Internet Explorer ou d'un robot d'indexation de contenu de Google.
- Le module Lightbeam de la Fondation Mozilla permet de prendre visuellement conscience de certaines opérations de traçage en ligne.
- HTTPS Everywhere, de l'Electronic Frontier Fondation, vise à faire transiter les communications de façon chiffrée dès que cette option est disponible et réduit ainsi les risques d'écoutes.
- Signalons aussi Self Destructing Cookies, qui permet de se débarrasser des cookies générés par une page dès que celle-ci est fermée évitant ainsi que ces cookies soient ultérieurement consultés.
- Pour les utilisat·rices plus avisé·es et prêt·es à réaliser les configurations nécessaires (souvent gérer les autorisations site de confiance par site de confiance), il est enfin recommandé d'utiliser uMatrix.

Pour aller plus loin :

- pour connaitre les traces basiques, mais nombreuses laissées lors des navigations : visiter le site What every Browser knows about you, le jeu en ligne Clickclickclick est aussi éloquent à cet égard.
- La page "contrôle tes données" gérée par la Quadrature du Net,
- un article d'Aeris sur son blog, Extensions Firefox pour protéger sa vie privée 2015-12-08,et de D. Crawford sur bestvpn en anglais, *The Complete Firefox Privacy and Security Guide*, sur les extensions relatives spécifiquement à la sécurité sur Firefox.

La plupart des extensions précédemment mentionnées, et notamment uBlock Origin permettent d'exclure ou d'inclure certains éléments du filtrage. On parle de "liste bloquée" ou de "liste autorisée". Ainsi, si on souhaite permettre à un site de nous tracer on peut choisir de désactiver le blocage sur ce site en particulier (liste autorisée).

> Pour cela cliquer sur le logo d'uBlock Origin et cliquer sur le "Symbole bleu" pour désactiver (ou réactiver) le blocage.

À l'inverse, si certains éléments ne sont pas automatiquement bloqués par les listes installées on peut les bloquer spécifiquement (liste bloquée).

> Pour cela, réaliser un clic droit sur l'élément souhaité et cliquer sur "Bloquer cet élément".

- Voir également la page de la CNIL « Maitriser mes données » sur son site cnil.fr.
- Pour comprendre le fonctionnement de Decentraleyes, voir leur Foire aux questions.

Sur la question du "Do Not Track", voir :

- la page du projet : donottrack.us (en anglais),
- une explication sur le site de l'EFF, "Do not Track" (en anglais),
- la page Wikipedia française "Do Not Track".

Fiche 06. Les mots de passe

L'usage de l'informatique implique souvent d'identifier les internautes. La technique la plus courante est basée sur le couple "identifiant/mot de passe". Selon les situations, l'identifiant peut être privé ou public, mais est souvent mal protégé. Le mot de passe est l'outil qui assure donc l'essentiel de la sécurisation. Si un individu mal intentionné obtient un mot de passe d'une personne, il pourra usurper son identité avec des conséquences potentiellement très graves (récupération des données, opérations commerciales, détournement de listes de contacts, etc.).

Les opérateurs qui demandent une identification doivent donc mettre en place de nombreuses mesures de sécurité pour gérer les mots de passe : dans les règles de création, dans la méthode de conservation, etc. C'est un enjeu très important, mais sur lequel on a peu de prise (si ce n'est d'éviter les opérateurs qui conservent et/ou transmettent les mots de passe en "clair" ou dont il est établi qu'ils sécurisent mal leurs données).

Côté utilisat·rice, il faut toutefois prendre des précautions.

La première précaution est d'utiliser un mot de passe qui ne soit pas facilement devinable par un attaquant (mots de passe basiques type 123456 ou azerty, date de naissance, identique à l'identifiant…), mais il faut également se prémunir des techniques de "force brute" consistant à tester automatiquement de très nombreux mots de passe. Pour réduire ce risque, il faut que le mot de passe soit suffisamment long (minimum 14 caractères) et comporte de la diversité : des minuscules, des majuscules, mais aussi des chiffres et des caractères spéciaux. Un opérateur sérieux mettra en place des mesures protectrices : nombre limité de tentatives, utilisation de "captcha"… Cela ne dispense pas pour autant de se protéger, car dans ces certains cas ces mesures ne seront plus opérationnelles (failles, récupération de la base de données chiffrée...).

Le problème reste que même une pratique numérique limitée implique d'avoir de nombreux comptes. Comme il est très important de diversifier ses mots de passe et de ne pas réutiliser le même pour tous les services, leur mémorisation devient vite complexe. Une conservation en clair sur post-it, dans un tableur ou un courriel est à l'évidence risquée.

Pour limiter ce problème de mémorisation, trois méthodes complémentaires sont disponibles :

- utiliser des "phrases de passe" facile à mémoriser, mais complexes à deviner,
- utiliser des méthodes d'identification mixtes,
- utiliser un gestionnaire de mot de passe.

6.1 Les "phrases de passe"

Plutôt que de devoir retenir des mots de passe complexes tels que "M9çT#411kl", on conseille d'adopter des "phrases de passe", plus simples à mémoriser tout en étant plus complexes à casser.
Il s'agit de retenir un assemblage de termes inspiré d'éléments connus de la seule personne concernée. Au lieu de la date et lieu de naissance on pourrait mettre "NéàdouzeH13 unmardi". Cette phrase peut être liée ou non au service utilisé (de façon non évidente) pour que l'on s'en souvienne. Pour une boite courriel par exemple : "HereJereçois~10mails/jour".
La phrase de passe permet de concilier les avantages d'un mot de passe complexe tout en le mémorisant plus facilement.

Même sur des services non critiques où une compromission du compte ne serait pas vraiment problématique (sans élément relatif à la vie privée, données bancaires, base de contact, etc.), il faut éviter d'utiliser le même mot de passe. Au minimum, on peut adopter une phrase de passe unique modulée pour chaque site avec

quelques variations non prédictibles. Il s'agit là d'un compromis avec le risque que la découverte d'un mot de passe entraine celle d'autres comptes (ex. si on est la cible particulière d'une attaque).

6.2 Les méthodes d'identification mixtes

Des opérateurs mettent à disposition des méthodes d'identification mixtes où un élément supplémentaire au mot de passe va être demandé à l'utilisat·rice. Pour les opérations importantes, l'identification se fait souvent avec un contrôle supplémentaire. Il s'agit fréquemment d'indiquer un code éphémère transmis par SMS.

La contrepartie de cette amélioration de la protection des comptes est la transmission de données supplémentaires (numéro de téléphone dans le cas précédent, validation par courriel, utilisation d'une carte à puce, mais des données biométriques peuvent aussi être utilisées dans des approches similaires). Attention toutefois cette méthode n'est pas infaillible et le vol du téléphone peut parfois paradoxalement permettre d'accéder au compte plus facilement.

Les méthodes mixtes sont très intéressantes en termes de sécurité pure. Il faudrait pouvoir s'assurer qu'elles soient bien mises en œuvre et que l'autre élément demandé n'implique pas d'autres risques. Ainsi accepter de communiquer son numéro de téléphone portable à une banque peut être justifié, fournir des données biométriques pour un achat en ligne est clairement disproportionné.

6.3 Les gestionnaires de mots de passe

Quelle que soit la manière dont on fabrique ses mots de passe, leur mémorisation est toujours un défi. Une solution est d'utiliser des gestionnaires de mots de passe qui offrent une protection sans effort de mémorisation.

Attention, toutes les solutions disponibles ne sont pas équivalentes. Ainsi, la quasi-totalité des navigateurs offre la possibilité d'enregistrer les mots de passe. Cette possibilité, si elle simplifie la vie, peut s'avérer dangereuse. Ce point est critique sur Firefox, mais aussi sur d'autres navigateurs où, par défaut, les mots de passe sont conservés en clair sans protection. Un mécanisme similaire existe au niveau du système sur Mac où, par défaut et sur simple validation de l'utilisat·rice, tous les mots de passe sont enregistrés dans un "trousseau".

Quiconque ayant accès au navigateur peut prendre connaissance de tous les mots de passe enregistrés. Pour pallier ce risque, il est préférable de ne pas y recourir. Si l'on ne peut s'en passer, il est absolument nécessaire de créer un "mot de passe principal" protégeant l'accès aux mots de passe enregistrés. Il faudra l'indiquer à chaque session ou accès, mais c'est une protection indispensable. La procédure est détaillée dans l'aide de Firefox.

> En bref, il s'agit d'aller dans "Préférences", onglet "Sécurité", "Utiliser un mot de passe principal", puis d'indiquer une phrase de passe.

Une meilleure solution est d'utiliser un gestionnaire extérieur. Ce logiciel, à installer sur son ordinateur, gèrera la mémorisation des mots de passe à notre place. Si les pratiques varient d'un logiciel à l'autre, les plus sérieux chiffrent les mots de passe qui ne deviennent accessibles qu'en fournissant le mot de passe maitre, le seul à devoir être mémorisé par l'utilisat·rice. Il doit être complexe et respecter les règles précédemment évoquées. Il sera ensuite possible de stocker tous les mots de passe, même les plus complexes, dans le gestionnaire sans devoir les mémoriser.
Le logiciel peut aussi proposer des mots de passe complexes (qu'il est tout de même conseillé de les modifier après génération, par précaution).

De nombreux gestionnaires sont disponibles; Lastpass, onepassword… En raison de sa gratuité, de sa relative praticité d'utilisation, du fait qu'il ait été audité et certifié par l'ANSSI comme sûr, et qu'il s'agisse d'un logiciel libre, le CECIL recommande le logiciel "Keepass" ou son "Fork"KeepassXC. Il s'agit de références en la matière.

Une pratique plus basique peut être de conserver ses passes peu utilisés dans une archive chiffrée en AES avec une phrase de passe solide.

Pour aller plus loin :

- l'ANSSI est l'Agence nationale de la sécurité des systèmes d'information, rattachée au Secrétaire général de la défense et la sécurité nationale. Elle "assure la mission d'autorité nationale en matière de sécurité des systèmes d'information". À ce titre elle préconise des règles de sécurisation des systèmes d'information pour le grand public,
- les recommandations de l'ANSSI sur les mots de passe qui ont toutefois certains défauts,
- une fiche pratique de la CNIL, *Sécurité : Comment construire un mot de passe sûr et gérer la liste de ses codes d'accès ?*,
- un tutoriel de la CNIL sur Dailymotion pour installer et utiliser Keepass,
- une fiche de la CNIL concernant le piratage de ses comptes sociaux *via* mot de passe ("prévenir, repérer et réagir"),
- quelques règles de base sur la création de mots de passe sur Ecrans.fr, *Choisir un bon mot de passe*,
- Zythom.blogspot.fr, *Cracker les mots de passe*, une présentation sur les méthodes "de base" permettant de casser des mots de passe pour comprendre ce dont il faut se prémunir,
- Quartz, Qz.com (en anglais), *A password like "adgjmptw" is nearly as bad as "123456"*, sur les séquences de mots de passe à éviter,
- NextInpact.com, *Ashley Madison : les mots de passe navrants de banalité*,
- NextInpact.com, Mots de passe : on vous aide à choisir le gestionnaire qu'il vous faut,
- Numerama.com, *Vos réponses aux questions secrètes ne sont pas si sûres, prévient Google*, sur les limites des questions secrètes pour la récupération des mots de passe,
- LeMonde.fr, *Le mot de passe, espèce en voie de disparition*, sur les velléités des constructeurs de remplacer les mots de passe par d'autres méthodes, notamment par des méthodes biométriques,
- Pour sortir des seules considérations de sécurité et de protection, voir les deux articles suivants du New York Times (en anglais), *The secret life of passwords*, et de Rue 89, *Dans mon mot de passe, il y a…*, qui révèlent tout l'intime et l'aspect émotionnel et poétique de certains mots de passe.

Fiche 07. Des outils alternatifs en ligne

Une nouvelle tendance se dessine. De plus en plus d'utilisat·rices ont recours à des services informatiques (ou "outils" : logiciels de bureautique...) situés à distance (et non plus sur leurs ordinateurs personnels) où sont aussi stockées leurs données. Si parfois un logiciel doit être installé pour communiquer avec l'outil, souvent un simple navigateur suffit.
On parle de *cloud computing*, en français "d'informatique en nuage". Ces services sont alors fournis par des prestataires.

7.1 Le "*Cloud computing*"

Les avantages pour l'utilisat·rice :

- il n'a pas toujours besoin d'installer, de configurer, de mettre à jour l'outil,
- ses données sont stockées sur un serveur extérieur, limitant les risques de perte de son propre fait,
- le service est accessible à partir de ses différents appareils (ordiphone, ordinateur, tablette...) et nécessite seulement un accès à Internet pour assurer les échanges 'ordinateur-service'.

De plus, ces services sont bien souvent gratuits. Mais pour rappel (fiche 5) : *"si c'est gratuit, vous êtes le produit !"*.

Les inconvénients pour l'utilisat·rice :

Ses données sont généralement exploitées à des fins de traçage publicitaire, d'établissement de profils de consommat·rices et l'utilisat·rice participe ainsi à créer de la valeur pour l'entreprise sans pourtant être rémunéré pour cela ! Par exemple, Google utilise les retranscriptions de Captcha pour confirmer son analyse des numéros des bâtiments.

L'expression "d'informatique dans les nuages" est trompeuse ; **le "nuage" est en réalité l'ordinateur de quelqu'un d'autre**. Les *datacenter* qui stockent les données appartiennent à des entreprises peut-être moins attachées au respect de la vie privée que leurs utilisat·rices.

L'informatique en nuage comporte donc de sérieux risques pour un particulier :

- perte de contrôle sur ses outils, par exemple avec l'impossibilité de les adapter à ses besoins,
- dépendance à un prestataire extérieur,
- ne pas pouvoir récupérer ses données pour les réutiliser dans un service concurrent,
- défaillance du prestataire,
- enfin, l'exploitation de grandes quantités de données donne du pouvoir à certaines grandes sociétés.

Pour lutter contre ces risques, le CECIL recommande quelques outils aux pratiques responsables qui sont d'excellents substituts à d'autres pourtant plus populaires.

Ainsi, dans la suite de cette fiche sont présentées des alternatives à de nombreux outils utilisables sur Internet, complétées par la fiche 8, dédiée à la gestion des courriels et la fiche 9, dédiée aux réseaux sociaux alternatifs.

7.2 Les outils alternatifs de travail collaboratif

Des outils ont été créés pour travailler collaborativement à distance. Il s'agit de logiciels de bureautique (édition de texte, tableur...), mais aussi d'outils plus spécifiques permettant de fixer un rendez-vous, sauvegarder des articles, discuter en ligne, etc.

Encore une fois, les grands acteurs d'Internet profitent de ces nouveaux usages pour obtenir un maximum d'informations personnelles sur les utilisat·rices et établir des profils commerciaux. Pour limiter ce traçage et ces atteintes à la vie privée, des solutions libres ont été créées que le CECIL recommande.

7.2.1 La dégooglisation d'Internet : les projets Framasoft.

L'association Framasoft, évoquée fiche 2, est particulièrement active sur cette question et cherche à mettre à disposition de tous (et notamment du public francophone) des outils fiables pour le travail collaboratif.

Elle met notamment à disposition :

- Framadate, basé sur le logiciel libre Studs qui est un outil de sondage permettant notamment de se mettre d'accord sur une date de réunion ou sur un choix en général. Il s'agit d'un parfait remplacement à "Doodle" qui trace lui les données personnelles de ses utilisat·rices et propose de la publicité,
- Framabag, basé sur le logiciel Wallabag qui permet de sauver facilement des pages Web pour une lecture différée et partagée entre plusieurs appareils. Il s'agit d'un parfait remplacement au service "Pocket",
- [Framaforms][https://framaforms.org/), s'appuyant sur Drupal, qui permetsX de réaliser facilement des questionnaires accessibles en ligne,
- Framapad, basé sur Etherpad un logiciel d'écriture collaborative de texte extrêmement performant qui permet de travailler simultanément sur le même texte,
- Framacalc, basé sur Ethercalc, un logiciel de tableur collaboratif.

Ces trois derniers services permettent aisément d'éviter d'utiliser Google Docs pour de nombreux usages.

Il existe même les services très demandés de partage d'images et de fichiers :

- Framapic, basé sur le logiciel Lutim pour partager des images,
- Framadrive, qui offre un hébergement synchronisé de fichiers pouvant être partagé entre différent·es utilisat·rices autour du logiciel Nextcloud. Un parfait remplacement à Dropbox !
- Framadrop, un service de partage de fichiers (anonymement et temporairement), basé sur le logiciel Lufi pour éviter de devoir recourir à un éditeur commercial où le respect de la vie privée et des données n'est pas garanti.

On peut également citer Framindmap, Framanews, etc. L'association en ajoute de plus régulièrement, tous méritent d'être découverts !

Pour Framasoft, il s'agit vraiment d'offrir des services efficaces et viables garantissant les libertés des utilisat·rices et sans exploitation de leurs données. Et en super bonus : Framatube/Peertube, une alternative décentralisée à Youtube !

7.2.2 D'autres services alternatifs

L'association Framasoft n'est, heureusement, pas la seule à offrir des services à distance respectueux des utilisat·rices.

Voici quelques autres services gratuits en ligne que le CECIL recommande :

- STUdS, qui est l'utilisation originelle du logiciel employé par Framadate,
- Etherpad est également hébergé par la Fondation Mozilla,
- Ethercalc, logiciel de tableur en ligne,
- le logiciel Jitsi permet d'héberger des vidéos et audio conférences. Il peut être installé sur un serveur personnel, mais son éditeur met aussi à disposition un service en ligne simple d'utilisation : Meet.Jit.si. Il s'agit d'une alternative valable à Skype ou à Hangouts (Google) garantissant la sécurité et la protection des conversations,
- le logiciel libre Nextcloud constitue une excellente alternative aux services de Dropbox. Comme précédemment indiqué il est mis en place par Framasoft avec Framadrive. Il fonctionne aussi parfaitement, avec plus de capacité, avec les hébergeurs évoqués dans la fiche 8 consacrée aux courriels (dont La Mère Zaclys et Ouvaton) chez qui il est offert par défaut. Il est très simple d'utilisation !
- Openstreetmap. Une cartographie éthique élaborée de façon collaborative et mise à la disposition de tous, librement et gratuitement. Openstreetmap est une alternative à promouvoir face à Googlemaps ou autres services commerciaux d'itinéraires (Mappy, ViaMichelin...). S'il nécessite un tout petit peu temps de prise en main et a encore quelques rares limites par rapport à ses équivalents commerciaux, ses potentialités sont bien plus grandes du fait de son appropriation possible par les utilisat·rices. Il est possible d'ajouter des informations et des calques personnels qui se superposeront à la carte. Il ne faut pas hésiter à l'utiliser voir même à en devenir contributeur : cela bénéficiera à tou·tes !

Pour aller plus loin :

- tous les logiciels libres présentés ici (Etherpad, Ethercalc) peuvent être installés sur un serveur personnel et ainsi limiter toute dépendance à une association ou une entreprise,
- une critique du *Cloud computing* par R. Stallman traduite sur le Framablog, *Ce que pense Stallman de Chrome OS et du Cloud Computing*,
- Degooglisons-Internet.org, le site de campagne de l'association Framasoft, qui indique les projets en cours pour éviter d'avoir recours à des services propriétaires gourmands en données personnelles,
- une interview sur Le Monde.fr de Gaël Musquet, cofondateur de la communauté d'Openstreetmap, *On peut créer des alternatives à Google avec le libre*,
- S'agissant d'Open Street Map, le site principal permet de calculer normalement un itinéraire, mais il existe aussi différentes interfaces dédiées : par exemple map.project-osrm.org, ou [GraphHopper.com](https://graphhopper.com/maps/
- pour une autre alternative à Skype, on peut citer les projets Tox.im, Ring.cx ou Mumble.

Fiche 08. Des hébergeurs de messagerie alternatifs : se réapproprier ses courriels.

Avoir une messagerie électronique est incontournable. Nos courriels sont le reflet de nos vies, le besoin de contrôle et de sécurité est donc primordial.
Pourtant, l'immense majorité des particuliers opte, par manque d'information, par facilité ou par habitude pour des services commerciaux des géants du Web : *Yahoo/Ymail*, *Microsoft/Hotmail-Live*, *Google/Gmail*, etc.
Ces sociétés disposent ainsi d'un pouvoir colossal en accédant aux données de connexion, voire aux contenus, des mails de très nombreux citoyens. Par exemple, Google scanne/ait le contenu des mails pour afficher des publicités corrélées. Les révélations d'Edward Snowden ont également prouvé l'existence d'une surveillance de ces services en "partenariat public-privé" avec des gouvernements.

Pour se protéger contre ces intrusions liberticides atteignant la vie privée, il faut essayer de quitter ces services. Malheureusement les solutions grand public équivalentes restent peu nombreuses. Il est difficile d'obtenir un service gratuit pécuniairement ou non qui garantirait réellement la vie privée et la sécurité de ses utilisat·rices et offrant les mêmes facilités.
Par exemple, Lavabit, a été contraint de fermer, car il refusait de livrer les mails de ses abonnés, dont E. Snowden, au gouvernement et à la justice américaine.

Il existe malgré tout de nombreux services de courriels en ligne "plus respectueux". Ces différentes solutions ont des limites, mais parmi les services gratuits (d'autres sont présentés en fin de fiche), le CECIL a retenu :
* Sud-Ouest.org (rien à voir avec le journal homonyme), hébergement associatif français à prix libre,
* [Netcourrier.com], hébergement privé français avec une offre gratuite limitée (500 Mo) et une offre à 12€/an bien plus développée
* Tutanota.com, hébergement privé allemand gratuit pour les particuliers,
* Autistici/Inventati, hébergement associatif italien militant gratuit avec une incitation à soutenir *via* une donation,
* ProtonMail.com, hébergement privé suisse avec une offre gratuite limitée et une offre payante plus développée de 48€/an.

Citons également quelques offres françaises d'hébergement respectueuses, dépassant la seule gestion des courriels (hébergement de sites, stockage de données à distance, listes de diffusion...) :

- l'offre associative de La Mère Zaclys,
- l'offre de la coopérative Ouvaton,
- l'offre commerciale de Gandi.

La plupart de ces solutions sont comparées sur les aspects sécurité et vie privée sur prxbx.com/email/.

Pour un usage classique de sa messagerie, toutes ces solutions sont fonctionnelles et garantissent un meilleur respect de la vie privée.

Il faudra choisir ! Certaines de ces offres ont un engagement militant plus important, d'autres une fiabilité pratique ou des caractéristiques différentes (quantité de stockage, diversités des usages possibles), les efforts en termes de sécurité ne sont pas tous égaux... La localisation de l'hébergement est également un critère important (les hébergeurs américains sont soumis aux règlementations liées notamment au Patriot Act, les hébergeurs français le sont à celles de la "loi renseignement". Il faut relever que l'hébergement en ligne à un cout, si on en a la possibilité, il est peut-être préférable de le payer pour "ne pas être le produit".

Ces solutions reposent souvent sur le logiciel libre RoundCube pour accéder à ses courriels sur le Web. Si on préfère gérer ses courriels en dehors de son navigateur, pour en disposer aussi hors connexion, ces solutions sont compatibles avec le logiciel de messagerie Thunderbird (accessible sur Gnu-Linux, Windows et Mac) que le CECIL recommande.

Une autre solution est d'installer son propre serveur local, sur un ordinateur dédié (permettant d'héberger un site Internet, un serveur mail...). Sans être trop complexe, cette solution demande toutefois des compétences techniques, un ordinateur dédié et une connexion fiable.

Force est de reconnaitre qu'il est difficile de quitter les services commerciaux peu respectueux si on s'y est habitué. Cela implique un changement d'adresse, un changement d'interface avec une potentielle perte de fonctionnalités, etc. Il s'agit pourtant d'une étape importante vers une meilleure protection.

Pour faciliter ce passage, un projet français essaye de proposer une messagerie sécurisée et respectueuse de la vie privée de ses utilisat·rices et disposant de fonctionnalités ambitieuses afin de convaincre le grand public. Il s'agit de CaliOpen, que le CECIL invite à découvrir, voire à soutenir.

Pour aller plus loin :

S'agissant des alternatives à l'hébergement des courriels :

- YunoHost une distribution Gnu-Linux, visant à faciliter l'installation d'un serveur personnel pour autohéberger ses services et, par exemple, ses courriels,
- La Brique Internet, une solution "clé en main" (matériel, logiciel et service) pour s'autohéberger, fournie par les associations membres de la Fédération FDN, des fournisseurs d'accès associatifs et militants.

D'autres hébergeurs de messagerie à découvrir :

- Posteo.de, hébergement privé allemand engagé sur les questions de protection des données à 12€/an.
- Toile-Libre.org, hébergement associatif français à prix libre,
- Vmail.me, hébergement privé français gratuit avec une incitation à soutenir *via* donation,
- le service mail de Riseup.net, hébergement militant américain gratuit, mais sur cooptation avec une incitation à participer *via* donation,
- KolabNow.com, hébergement privé suisse payant offrant de garanties conséquentes concernant la vie privée.

Fiche 09. Des réseaux sociaux alternatifs

9.1 Promouvoir et défendre des réseaux sociaux respectueux des utilisat·rices

Il ne semble pas nécessaire de rappeler les dangers potentiels de Facebook pour les libertés tant ceux-ci sont documentés, et ce même si on configure correctement son compte. Un téléchargement de ses données devrait permettre de s'en convaincre, si nécessaire.

Voir par exemple les explications du site sortir de Facebook, InternetActu.net, "*la vie privée un problème de vieux cons ?*"... et ce même pour les utilisat·rices non-inscrit·es à Facebook.

Pour un internaute qui utilise fréquemment un réseau social, en changer est loin d'être évident. En effet, l'intérêt de tels réseaux est directement lié au nombre d'inscrit·es. Ainsi, à service équivalent ou même supérieur, beaucoup préfèrent rester sur Facebook, Twitter, Snapchat, Instagram, Youtube, etc. où sont présentes un grand nombre de leurs connaissances, plutôt que de migrer vers un autre réseau plus respectueux.
Cela ne doit pas servir d'excuse, critiquer les dangers de Facebook tout en continuant d'y participer, en dévoilant sa vie privée et en travaillant bénévolement pour cette société sans chercher d'alternative a ses limites.

Pour ceux et celles convaincues de l'intérêt des réseaux sociaux, mais qui souhaitent lutter contre cette hégémonie des "réseaux publicitaires" et utiliser des services plus respectueux des libertés, le CECIL recommande les alternatives suivantes.

9.2 Mastodon, une alternative décentralisée à Twitter

Twitter est un outil performant, qui dispose d'une importante communauté facilitant la transmission d'informations ciblées, permettant de signaler facilement des articles pertinents et faire connaitre des évènements. Le statut public, par défaut, des *Tweets* limite les risques liés à une croyance dans le caractère secret de ceux-ci. Attention toutefois, ce fonctionnement public peut conduire à un changement d'échelle radical dans la diffusion des tweets.
De plus, cette entreprise collecte les données personnelles et les messages de ses utilisat·rices et les exploite commercialement à des fins de traçage, de revente massive et d'établissement de profils commerciaux. Si l'entreprise semblait un peu plus respectueuse que ses deux grandes sœurs, Facebook et Google, son usage conséquent lui confère malgré tout beaucoup de pouvoir et elle exploite tout autant les données personnelles.

Pour qui souhaiterait limiter ce pouvoir, des alternatives plus respectueuses existent :

- Identi.ca (s'appuyant sur le logiciel libre pump.io),
- SeenThis.net.
- Et surtout Mastodon

Si les deux premiers réseaux ont leurs intérêts, force est de reconnaitre qu'ils ne constituent pas encore une alternative complètement fonctionnelle, mais doivent être soutenus.

Créé fin 2016, Mastodon a toutefois réussi à réaliser une véritable percée en développant un véritable réseau social libre et décentralisé. En effet, le logiciel Mastodon, permet d'installer une instance qui sera fédérée aux autres instances indépendantes sur le "Fediverse". Une instance est une implantation nouvelle du logiciel

maintenue par un particulier, une entreprise, une association, avec plus ou moins de rigueur quant au suivi des mises à jour, la modération, la stabilité du service, etc. Il existe de nombreuses d'instances plus ou moins grandes et sur chacune, les gestionnaires de l'instance fixent les règles.
À l'instar des courriels, les membres d'une instance peuvent discuter avec celles et ceux d'autres instances et suivre leurs messages.
Le logiciel est libre, décentralisé le réseau peut perdurer même si l'une des instances rencontre un problème, la multitude d'instances qui ont été créées évite de rendre les participant·e·s au réseau dépendant d'un seul prestataire et peuvent choisir une instance conforme à leurs valeurs, la quasi-totalité des instances ne diffuse aucune publicité ni ne trace leurs membres. Cerise sur le gâteau les "pouets" (équivalents des *tweets*) peuvent faire 500 caractères et être précédés si besoin d'un avertissement relatif au contenu si celui-ci est susceptible d'être problématique.

L'intégralité du Fediverse a dépassé le million de membres et continue de croitre.

Pour le rejoindre, il faudra choisir une instance. Il est possible de les découvrir sur cette page : https://joinmastodon.org/#getting-started

Le CECIL recommande autrement ces différentes instances : Mamot.fr, l'instance de l'association La Quadrature du Net, Framapiaf, celle de Framasoft ou encore Mastodon.xyz, gérée par The Kinrar sur laquelle est inscrite le compte du CECIL : @Cecil@Mastodon.xyz

9.3 Diaspora, une alternative à Facebook

Le logiciel Diaspora est une alternative à Facebook. Il s'agit d'un logiciel libre, développé par la fondation Diaspora sans but lucratif et a dans sa construction même la volonté de protéger la vie privée.

Ses trois concepts clés sont la décentralisation, la liberté et la confidentialité.

L'originalité de Diaspora est qu'il s'appuie sur de nombreux petits serveurs sur lesquels les données vont être réparties de façon chiffrée.
On peut participer à ce réseau sans connaissance particulière en utilisant n'importe lequel des points d'inscription (appelés Pod) disponibles sur podupti.me.

Si l'on souhaite même éviter que ses données soient hébergées par un tiers, Diaspora permet de stocker ses propres données sur son serveur personnel (ce qui demande toutefois une compétence technique non négligeable).
De cette structure en réseau découle la multiplication des serveurs d'hébergement de Diaspora.

Les paramètres du logiciel permettent de gérer facilement ses propres critères de diffusion (quel public, durée de visibilité...), l'outil est fluide et pratique. Sa seule limite est son faible nombre d'utilisat·rices acti·ves. En rejoignant ce réseau et en invitant ses amis à en faire de même on peut toutefois changer cet état de fait et continuer de bénéficier de cet outil sans voir ses données offertes en pâture aux publicitaires, aux *data brokers* et à la surveillance des États.

Le CECIL recommande d'utiliser et de soutenir le Pod de l'association Framasoft évoquée par ailleurs, qui s'appuie sur Diaspora : Framasphere.org.

N'hésitez pas : inscrivez-vous !

Pour aller plus loin :

- TOSDR.org, un projet révélant les dispositions positives ou problématiques des conditions d'utilisation de différents services en ligne permettant, par exemple, de découvrir les dispositions problématiques des réseaux sociaux publicitaires,
- Nextinpact.com, **Mastodon : mais en fait, comment ça marche ?**,
- à noter qu'il existe un autre logiciel décentralisé de réseau social similaire à Diaspora : Movim.eu,
- Zinc, le réseau social du MondeDiplo s'appuyant sur SeenThis.

Fiche 10. L'anonymat sur Internet

"Sur Internet, personne ne sait que vous êtes un chien". Cet ancien adage d'Internet était peut-être pertinent en 1993, actuellement la situation est plus complexe. S'il reste possible d'utiliser un pseudo séparé de nos autres identités pour discuter ou commenter et choisir son identité selon le contexte, on n'est pas pour autant anonyme. Quand on navigue sur Internet, on laisse un grand nombre de traces. Parmi elles, l'adresse IP de l'ordinateur et d'autres informations qui permettent d'être identifié.

Ainsi, par défaut, chaque accès à des services sur Internet est enregistré ("*loggé*") par différents acteurs (fournisseurs d'accès Internet, services auxquels on se connecte, éventuels acteurs intermédiaires...). Le fournisseur d'accès disposant normalement de l'identité civile de la personne titulaire de la connexion, il peut (et y est contraint dans certains cas) la livrer à une autorité accompagnées des différentes données de connexion (métadonnées) dont il dispose. Tout ordinateur transmet aussi automatiquement à tous les services en ligne un certain nombre d'informations (dont le *user-agent* qui correspondent aux données transmises par le navigateur indiquant le système d'exploitation, le navigateur, etc.) qui peuvent permettre de l'identifier.

Pourtant, bien que la possibilité d'une forme d'anonymat puisse engendrer des problèmes (commentaires malveillants, insultes ou menaces, etc.), ce peut être le seul rempart contre des sanctions injustes pour avoir exprimé une opinion différente ou s'être renseigné sur des sujets sensibles. Il existe de très nombreuses raisons légitimes pour ne pas souhaiter que ses navigations sur Internet soient reliées à son identité civile : protection contre une surveillance abusive (qu'elle soit privée ou publique), échanges protégés dans le cadre de professions ou activités sensibles (avocat·e, journaliste, militant·e, lanceu·se d'alerte)... et ne serait-ce que la volonté de ne pas être perpétuellement suivi·e et épié·e.

Des outils existent pour protéger ses identités et participer ainsi à renforcer la liberté d'expression et d'opinion. Le principe est de faire transiter ses communications de façon sécurisée par un autre serveur qui accèdera à notre place aux contenus désirés. On empêche ainsi le service final ou tout autre intermédiaire de connaitre la provenance de la connexion.

C'est notamment le fonctionnement d'un proxy ou d'un Réseau privé virtuel (ou *VPN*), mais c'est aussi le principe de base d'un réseau comme "TOR" destiné à protéger les communications.

10.1 Usage du réseau Tor

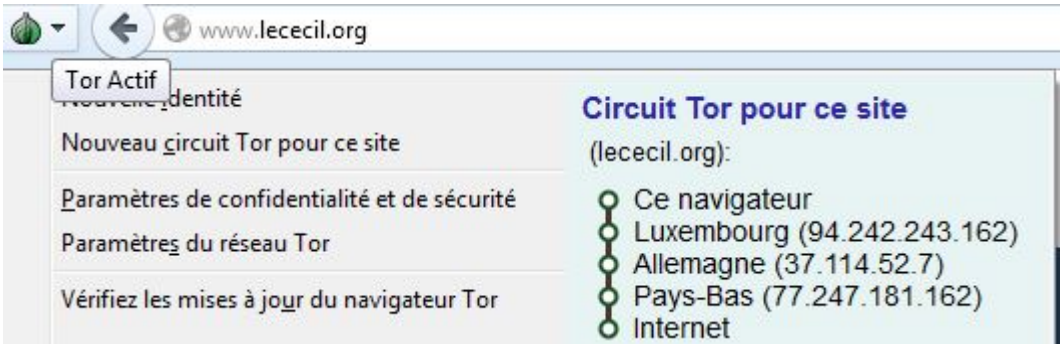
Qui s'intéresse un peu à la protection de la vie privée sur Internet a sans doute déjà entendu l'acronyme "TOR" sans pour autant forcément savoir ce dont il s'agit.

En pratique, Tor (*The Onion Router*, le "routage en ognon") est un réseau informatique qui s'appuie sur de nombreux routeurs, appareils et serveurs qui vont assurer automatiquement la redirection des "paquets de données", donc des communications sur Internet. La multiplicité de ces routeurs, servant de couches de protection, rend extrêmement difficile de retracer leur provenance. Pour cette raison, il est souvent critiqué par les autorités et services policiers.

Il est développé par le "projet Tor" qui a pour objectif :
"d'améliorer les droits de l'homme et les libertés fondamentales en créant et déployant des techniques libres et ouvertes protégeant l'anonymat et la vie privée, en soutenant leur usage et leur disponibilité inconditionnelle et en encourageant leur compréhension scientifique et populaire" (traduction CECIL).

Son objectif principal est de protéger l'origine d'une connexion sur Internet et donc de favoriser l'anonymisation des communications sur Internet. Ainsi, une requête à un serveur va transiter par de nombreux ordinateurs ou serveurs répartis dans le monde empêchant normalement l'hébergeur final ou à une organisation surveillant un point précis du réseau (telle que la *NSA*) de savoir qui est l'auteur de cette requête. Pour simplifier un peu, au lieu de l'adresse IP de l'auteur de la requête, c'est celle d'un nœud réseau Tor qui sera détectée rendant l'identification ou toute tentative de traçage extrêmement difficile.

À titre d'exemple, un circuit Tor classique pour accéder à un site ressemblera à cela :



10.1.1 Pourquoi utiliser Tor ?

Ainsi, Tor complique considérablement la tâche pour identifier qui accède à quoi, qui recherche quoi, qui transmet quoi à qui, etc. Même les sites consultés sont incapables d'identifier le véritable auteur de la requête.

Cela peut s'avérer nécessaire et être ainsi utile à :

- toute personne pour préserver sa vie privée et son intimité ;
- tout·e professionnel·le pour favoriser la confidentialité d'échanges d'informations ;
- des lanceu·ses d'alertes et des journalistes pour se protéger et informer depuis des zones dangereuses, sans risques de censure par certains pays ou opérateurs ;
- éviter d'être identifié dans des pays peu démocratiques et potentiellement torturé ou tué pour ses connexions en ligne ;
- des militaires pour garantir l'intégrité de l'information ;
- contourner des formes de censure ou de territorialisation des informations ;
- etc.

Même si on se soucie peu de protéger sa vie privée, utiliser Tor sans réel besoin d'anonymat, protège indirectement celles et ceux qui l'utilisent par nécessité en faisant ainsi grossir "la botte de foin" : en évitant que leurs communications sortent du lot.

10.1.2 Comment utiliser Tor ?

La croyance commune est qu'il est difficile d'utiliser Tor, qu'il s'agit d'une pratique de spécialiste... ce n'est pas le cas. Utiliser Tor c'est aussi simple qu'utiliser n'importe quel navigateur.

Il suffit de télécharger le navigateur Tor, *Tor Browser*, qui est disponible pour tous les systèmes d'exploitation et de l'installer sur son ordinateur ou même sur une clé USB.

À partir de là on peut naviguer sur Internet *via* le réseau Tor sans autre opération !

Sur la page d'accueil, cliquer sur "Tester les paramètres du réseau Tor" pour vérifier que tout est fonctionnel.

Félicitations. Ce navigateur est configuré pour utiliser Tor.

Votre adresse IP semble être : **176.10.99.200**

C'est donc loin d'être une opération de spécialiste : c'est accessible à tou·tes ! Une autre croyance courante est celle de la lenteur problématique du réseau TOR. Si cela était pour partie vrai il y a quelques années, grâce à de nombreux acteurs (tels que l'association Nos oignons en France) le réseau reste suffisamment fluide pour un usage basique d'Internet !

10.1.3 Les limites

Même si aucun élément ne permet de penser que la sécurité de Tor soit actuellement compromise (voir les liens présentés en fin de fiche), le réseau n'offre pas pour autant une garantie absolue d'anonymat, mais, bien utilisé, une amélioration substantielle de la protection de l'origine des communications. Au-delà de failles pouvant être découvertes dans le futur, certaines mauvaises pratiques peuvent toutefois révéler une identité par :

- la transmission d'informations, personnelles ou non lors des navigations (utilisation du même pseudo ou mot de passe, syntaxe similaire...) ;
- l'utilisation de modules ajoutés ou de logiciels tiers (flash, java, extensions de navigateur...) ;
- l'ouverture de documents téléchargés *via* le *Tor Browser*, en étant encore connecté qui peuvent accéder à des documents sur le réseau (et ainsi transmettre la véritable adresse IP et données d'identification).

Enfin, si on utilise Tor pour communiquer directement avec d'autres personnes, d'autres précautions sont nécessaires pour protéger son identité et ses communications.

Utiliser Tor ne permet donc pas de tout faire si l'on souhaite protéger fortement son anonymat et n'est pas adapté à tous les types d'utilisation : pas de contenus "flash", pas de téléchargement massif ni "pair à pair", des limites possibles sur les flux vidéos, une absence d'identification durable sur les sites consultés (mais c'est le but), une personnalisation des sites (langage, etc.) dépendante du dernier nœud réseau avant la requête, etc.

Il faut noter que si le dernier nœud par lequel les communications transitent est malicieux, il pourra intercepter l'intégralité du trafic si la communication n'est pas chiffrée. Il faut donc être très prudent en ne transmettant *via* Tor que des informations chiffrées (par le *HTTPs*).
Il faut toutefois relever qu'une chercheuse en sécurité a utilisé une méthodologie pour déterminer l'existence de serveurs Tor malicieux et dans son étude, seules 6 sorties Tor sur 1500 se sont révélées problématiques.

De plus, si quelqu'un·e est ciblé·e directement par une surveillance de son réseau local ou de son ordinateur (infecté par un virus par exemple) l·a surveillant·e connaitra toutes ses communications.

10.1.4 Les "services cachés"

Le réseau Tor permet d'accéder aux différentes pages Web. Mais en plus, les différents routeurs et serveurs qui permettent de naviguer *via* Tor peuvent aussi venir héberger des pages et des services de messagerie instantanée. Cet hébergement est protégé par le réseau Tor et uniquement accessible par ce biais, il n'est guère possible d'identifier le propriétaire. Cette fiche n'a pas pour objet de détailler comment héberger de telles pages qui vont être identifiées par une adresse finissant en .onion, mais il est possible de le trouver sur la page du projet Tor.

Si des pages peu respectueuses des lois françaises sont accessibles par de telles adresses (exemple : *"The Silk Road"*), en même temps cela permet également à des dissident·es politiques de pays peu démocratiques d'échanger et de transmettre des informations.

À titre d'exemple, une fois le *Tor Browser* lancé, essayer :

- 3g2upl4pq6kufc4m.onion/ qui renvoie vers DuckduckGo sur Tor ;
- torlinkbgs6aabns.onion/, ou zqktlwi4fecvo6ri.onion/ qui sont des listes de liens ".onion" que l'on peut trouver dans ces services cachés.

10.1.5 Les autres réseaux anonymisant

Il existe d'autres initiatives similaires à Tor qui disposent d'autres atouts ; elles offrent aussi des bonnes garanties d'anonymat et peuvent même avoir un intérêt supérieur à Tor, mais elles n'ont pas le même degré d'aboutissement ou de qualité de service. Le CECIL propose toutefois de découvrir :

- I2P pour "*Invisible Internet Project*", qui combine un fonctionnement proche de Tor et une approche en "pair-à-pair". Il permet ainsi le téléchargement de fichiers et l'établissement de communications anonymes. Grâce à I2P deux ordinateurs peuvent communiquer entre eux (*via* des intermédiaires), plus simplement que sur Tor, sans que l'un puisse identifier l'adresse IP de l'autre.
- Freenet, qui fournit des services similaires, mais est plutôt axé sur la publication de documents décentralisés ; ainsi si une personne met un document sur Freenet celui-ci va se retrouver hébergé, découpé en différents morceaux, sur de nombreux serveurs et ne pourra plus être supprimé tant que le réseau existe et ce même si l'auteur y était contraint.

Ces deux services ne nécessitent que d'installer un logiciel pour les essayer et se faire sa propre opinion.

10.2 Usage d'un VPN

Acronyme anglais de "réseau privé virtuel", un VPN (*Virtual Private Network*) est une technique permettant de créer un lien réseau direct, un "tunnel" entre deux ordinateurs éloignés. Ainsi quand un ordinateur est connecté à un VPN, il peut accéder au réseau "au travers" d'un autre, qui, aux yeux du réseau, sera celui qui réalise les opérations. Cela permet par exemple de se connecter à distance au réseau interne (*intranet*) d'une entreprise, mais aussi d'accéder à Internet sans que l'adresse IP de la personne qui utilise le VPN soit enregistrée. Seules l'adresse IP et les caractéristiques techniques du serveur offrant le VPN circuleront sur le réseau.

Des entreprises proposent des solutions de VPN qui vont protéger la confidentialité de l'origine des communications. En souscrivant à leurs services, si la communication en direction du VPN est sécurisée (chiffrement...), il sera très difficile de déterminer qui a accédé à tel ou tel contenu sur Internet, les informations d'identification transmises étant celles du VPN de l'entreprise.

Le niveau de sécurisation est fonction de l'entreprise. Il faut donc qu'elle présente certaines garanties. Tout dépend des besoins. Ainsi, si le seul objectif est d'éviter que les services utilisés puissent "profiler" l'adresse IP, la plupart des solutions existantes sont convenables.

Dans l'hypothèse d'un service qui utilise l'adresse IP pour localiser l'internaute, par exemple certaines vidéos dont l'accès est restreint aux résidents d'un pays, l'usage d'un VPN localisé dans ce pays peut permettre de se soustraire à cette contrainte.

S'il y a absolument besoin qu'une communication ne soit pas tracée jusqu'à son émetteur par les autorités, l'immense majorité des VPN ne seront pas adaptés. En effet, ces entreprises restent soumises aux lois nationales. Elles doivent respecter les mandats judiciaires de transmissions de données d'identification. Les garanties de confidentialité offertes par un VPN sont dépendantes non seulement de la localisation de l'entreprise et de ses serveurs, mais aussi de ses conditions contractuelles et de sa bonne volonté à coopérer avec les autorités publiques. Face à ce risque de surveillance, le CECIL ne saurait faire une recommandation précise (sans possibilité d'auditer véritablement ces services ni de tester toutes les solutions).

Il existe de très nombreux services et comparatifs de services. Offrir un tel service a un cout, il faut donc se méfier des services "gratuits", dont la rémunération est indirecte (publicité, produit d'appel, utilisation des données à d'autres fins...). Il existe toutefois quelques services gratuits aux caractéristiques limitées (en bande passante, en débit général, en protocoles disponibles...) qui apparaissent comme fiables si l'objectif est seulement de se protéger des entreprises commerciales. On peut aussi citer des VPNs issus d'organisations sans but lucratif ayant pour vocation de protéger la vie privée :

- Arethusa limité toutefois à la seule navigation Web dans sa version gratuite ;
- Autistici, au débit toutefois très limité ;
- RiseUp, accessible sur seule cooptation ou acceptation sur demande.

Pour les solutions payantes plus complètes, sans pouvoir faire de recommandations précises voici les points qu'il est important de prendre en compte :

- les garanties techniques : stabilité de l'infrastructure, du service, nombre de serveurs et répartition sur le globe, etc. ;
- les logiciels et protocoles utilisés, il faut ainsi s'assurer qu'il s'agisse d'un logiciel fiable, principalement "OpenVPN", sous licence libre et qui semble faire ses preuves en termes de sécurité ;
- la localisation juridique de l'entreprise et de ses serveurs qui conditionne la législation à laquelle elle est soumise et donc aux potentielles demandes des États concernés ;
- les garanties juridiques en termes de vie privée présentes dans les conditions commerciales.

Il faut bien prendre le temps d'analyser le service et d'en connaitre les limites, un VPN sérieux protègera contre la surveillance privée et évitera les méthodes liées à la seule surveillance du réseau (*IP-tracking*, limites liées à la localisation de l'adresse IP, surveillance automatique des connexions de "pair à pair"...), mais ne constituera pas une garantie absolue contre des demandes étatiques ou judiciaires d'identification de connexion.

Pour aller plus loin :

Sur Tor

- Le site officiel de Torproject.org
- Télécharger le *Tor Browser* (ou navigateur Tor)
- Une description exhaustive des usages légitimes de Tor torproject.org/about/torusers.html (en anglais)
- Il est possible de se protéger d'une compromission de son ordinateur en utilisant Tor *via* le système d'exploitation Tails utilisé en Live-Usb.

- Pour soutenir le développement de nœuds Tor et ainsi renforcer le réseau, il est possible en France de participer à l'association "Nos Oignons"
- Une vidéo de présentation de Tor (sur Youtube), Navigation anonyme avec Tor Browser - TechTour : Démo
- A. Guiton, Liberation.fr, Tor : Mails-toi de tes oignons
- Lundi.am, Utiliser Tor contre la Loi Renseignement ? Réponses avec Lunar, membre du projet Tor
- The Guardian (en anglais), NSA and GCHQ target Tor network that protects anonymity of Web users, s'appuyant sur des documents dévoilés par E. Snowden témoignant que si la NSA souhaiterait pouvoir "désanonymiser" les communications du réseau Tor, jusqu'ici elle semble ne pas y être parvenue. Les documents dévoilés de l'entreprise *The Hacking Team* témoignent du même état de fait
- J. Bearman, sur Wired (en anglais), The Untold Story of Silk Road, un récit captivant en 2 parties conséquentes retraçant l'histoire du site *The Silk Road* et de son supposé créateur Ross Ulbricht alias *Dread Pirate Robert*
- lemagtechno.com, Réseau anonyme lequel choisir, un rapide comparatif (en français) de I2P, Tor et Freenet de ces trois services.

Sur les VPN

- Vpnblog.net dispose de nombreux comparatifs et analyses sur les VPN qui semblent fiables, attention toutefois de nombreuses comparaisons de VPN sont uniquement promotionnelles et loin d'être objectives.
- Une analyse un peu ancienne (2011) des garanties concernant la vie privée de nombreux VPN chez Torrent Freak, traduite par Torrent News en français, Quels fournisseurs de VPN prennent vraiment l'anonymat au sérieux ?
- Parmi les VPN payants les plus communément cités comme techniquement fiables (pas forcément juridiquement) on trouve notamment IPVanish.com, localisé aux États-Unis, qui revendique ne pas conserver de logs, on peut aussi citer le français Toonux.net engagé dans la protection de la vie privée, mais aux possibilités techniques plus limitées (pas de choix de pays de sortie par exemple) ou Ipredator.se, une solution VPN co-fondé par Peter Sunde un des fondateurs de The PirateBay.
- L. Adam, ZDnet.fr, Controverse autour de la sécurité des VPN grand public, suite à une étude critiquant la sécurité des principaux VPN payants
- Attention, une faille dans un des protocoles de communication (WebRTC) a été découverte début 2015 et peut dévoiler l'identité de l'utilisateur d'un VPN. Les indications pour s'en défaire son disponible sur Numerama, Vous utilisez un VPN ? Une faille dévoile votre adresse IP réelle
- Desgeeksetdeslettres.com, La différence entre un proxy et un VPN, qui revient aussi sur les limites des deux outils

Plus d'information sur l'anonymisation en général :

- Un excellent article de The Intercept (en anglais), Chatting in Secret While We're All Being Watched, qui combine à la fois les explications sociétales sur les "besoins" de communiquer anonymement et des explications pratiques sur "comment" par le biais du chiffrement et de l'usage du réseau TOR
- Une rapide présentation sur itpro.co.uk (en anglais), **Security researchers develop anonymous Web browsing**, d'un projet de recherche d'une solution similaire à Tor pour garantir l'anonymat sur Internet
- Un article de GoldenFrog.com une entreprise proposant des solutions commerciales, **Myths about VPN logging and anonymity**. L'article est très partial, mais présente bien les limites de la recherche de confidentialité / d'anonymat et les fausses promesses à ce niveau

Fiche 11. Le chiffrement des données

Une très large part de nos vies est "numérisée". Nos écrits, nos communications et échanges sont transformés en "bits" (0 ou 1), afin de pouvoir être interprétés et exploités par les ordinateurs, mais aussi stockés sur des mémoires informatiques et transmis *via* les réseaux.

Ces techniques offrent d'énormes capacités de stockage et de communication, mais elles ont leur revers. Elles facilitent l'intrusion par quelqu'un · de mal intentionné ·e. S'il importe de limiter ses traces et de protéger ses informations confidentielles, cela reste insuffisant.

Heureusement, il existe des méthodes, issues notamment des mathématiques, qui, bien employées, permettent de protéger ses données et ses communications en les rendant incompréhensibles, sauf de soi et de ses correspondants.

11.1 La cryptographie : protéger ses données par le chiffrement

L'idée générale est de "brouiller" le contenu des données par des méthodes mathématiques. On parle alors de "cryptographie" ou le secret des écrits, dont les applications permettent le **chiffrement** des données et des communications. Un exemple très connu : la méthode dite du "chiffre de César", qui est une forme de chiffrement simple : chaque lettre du message est remplacée par une autre selon un nombre de décalages choisi (qui servira de code). Avec un décalage de 5 le A devient F, le B devient G, etc. BONJOUR devient GTSOTZW.

L'objectif des outils présentés ci-après est analogue : rendre des données incompréhensibles si l'on ne connait pas le code. Évidemment, le "chiffre de César" est une technique très rudimentaire et facile à décrypter (à déchiffrer sans connaitre le code). Les outils présentés dans cette fiche mettent eux en jeu des techniques bien plus complexes où la méthode de chiffrement est publique, donc analysable par une personne compétente pour s'assurer qu'il n'y a pas de faille, mais où, sans connaissance du code utilisé, il est quasiment impossible pour un attaquant de décrypter les données. Attention, le simple échange de données chiffrées est en soi une information.

Sans trop entrer dans les détails, le CECIL propose deux fiches sur le chiffrement pour éviter les mauvaises pratiques. L'objectif principal y est de présenter des outils majoritairement considérés comme fiables.

Cette fiche présente les outils permettant de chiffrer **ses données stockées**. La suivante explique comment protéger **ses communications** par chiffrement.

11.2 Chiffrer ses données stockées

Pour améliorer la sécurité et la confidentialité de ses données et documents, les chiffrer est une bonne pratique. Sans protection, ces données peuvent être consultées par quiconque peut y accéder, par exemple par l'insertion d'une clé USB, le vol d'un ordiphone, la récupération du disque dur ; les simples protections d'accès à la machine (mot de passe de session, schéma de déblocage...) sont insuffisantes. De même, si ces données sont conservées ou sauvées sur un serveur extérieur (dans le "nuage"), elles sont aussi accessibles à ceux qui y ont accès (notamment l'entreprise qui gère ce service).

11.2.1 Chiffrer tout ou partie d'un disque dur ou d'un périphérique de stockage

Gnu-Linux

Pour l'utilisat·rice d'un système d'exploitation Gnu-Linux récent (Ubuntu, Linux Mint, Tails, Kali...), c'est très simple : à l'installation un choix est proposé de chiffrer intégralement le disque dur ou le dossier personnel (*via* le logiciel dm-crypt avec LUKS). Pour un usage personnel classique, le CECIL conseille vivement de chiffrer son disque dur ou, si l'ordinateur est partagé, au moins le dossier personnel avec un code fiable (telle une phrase de passe). Ce code protègera l'accès à la session (un minimum vital) et le déchiffrement des données.

Windows et Mac OS X

Pour Windows ou Mac OS X, il faudra télécharger un logiciel. En effet, ceux préinstallés (BitLocker pour Windows, Filevault pour Mac) sont "propriétaires", ils ne peuvent donc être audités et sont donc susceptibles de comporter des failles ou portes dérobées.

Le CECIL recommande donc un logiciel libre : **Veracrypt**

> Une fois téléchargé, puis installé et lancé en suivant les instructions, cliquer sur "*Create Volume*", puis sur "**Encrypt the system partition or entire system drive**" et continuer à suivre les instructions selon les spécificités.
> La procédure n'est pas complexe, mais il est important de ne pas se tromper et il est préférable d'avoir une sauvegarde de ses données.

Des tutoriels très bien décrits sont disponibles sur le site Nextinpact - VeraCrypt : comment chiffrer et cacher un OS complet.

Pour Mac OS X, il n'est pour le moment pas possible de chiffrer tout le système avec Veracrypt, il faudra pour cela utiliser le logiciel AESCrypt

Dans le cas où Filevault serait malgré tout utilisé, il faut faire attention à l'utiliser correctement, voir pour cela les explications sur le site securitemac.com.

11.2.2 Chiffrer certains fichiers ou dossiers

Dans la partie précédente, l'objectif était de chiffrer tout ou partie d'un disque dur ou un périphérique de stockage, selon la situation (ordinateur partagé, etc.), cela peut être inadapté ou contraignant. Il existe des logiciels permettant de ne chiffrer que certains fichiers particuliers et sensibles. Le CECIL recommande le logiciel libre 7zip, adapté aux trois systèmes d'exploitation, qui permet de réaliser rapidement des archives compressées et chiffrées de documents *via* la méthode AES256 considérée comme fiable.

- Pour les distributions Gnu-Linux, il est généralement installé par défaut sous le nom de p7zip :

> Pour l'utiliser, il suffit de sélectionner les fichiers ou dossiers à protéger, de réaliser un clic droit et de cliquer sur "Compresser". Il faut ensuite choisir l'emplacement de destination de l'archive et une phrase de passe.

L'archive produite sera ainsi chiffrée. Il faudra par contre penser à supprimer complètement les fichiers originels qui sinon resteraient accessibles. Si le besoin en sécurité est important, il faut aussi s'assurer qu'ils ne seront pas récupérables en utilisant un logiciel de nettoyage tel que Bleachbit.

- Pour Windows, pour utiliser 7zip :

  Après avoir téléchargé le logiciel, l'installer en conservant les options par défaut qui l'intégreront au menu contextuel (accessible par clic droit sur un fichier ou un dossier).
  Sélectionner ensuite les fichiers à chiffrer, un clic droit -> "7-zip" -> "Ajouter à l'archive"
  Dans la fenêtre qui s'affiche choisir le code de chiffrement, le chiffrement AES 256 et cocher "Chiffre les noms de fichiers" si cela a une importance et "Effacer les fichiers après compression".

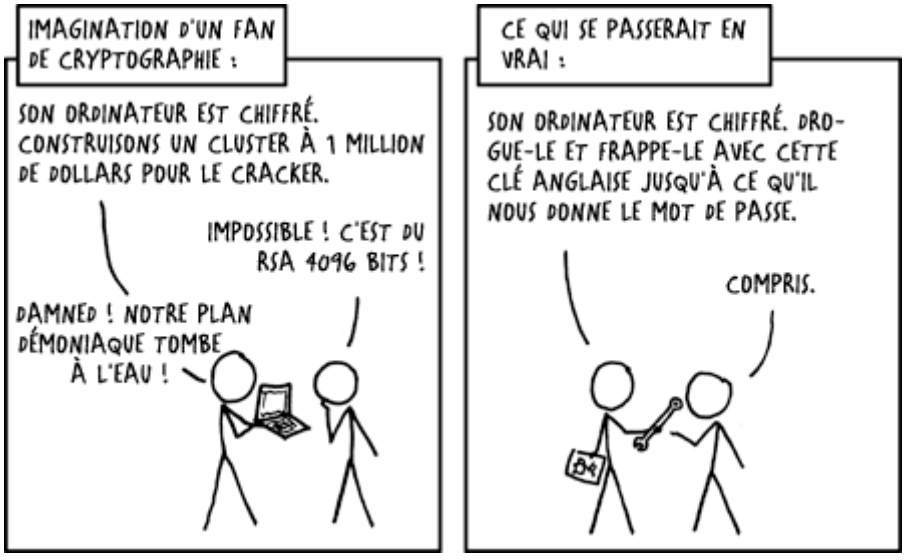
- Pour Mac OS X, il s'agit du logiciel 7zx.

11.3 Limites au chiffrement des données

Attention même si actuellement ces méthodes sont considérées comme fiables, pour autant elles ne sont pas infaillibles :

- failles encore non détectées, portes dérobées,
- dépendance dans le système d'exploitation propriétaire qui aura accès aux données,
- présence d'un virus, d'un enregistreur de frappes espion, d'une surveillance directe de l'ordinateur,
- augmentation constante de la puissance de calcul,
- etc.

Elles ne protègent surtout pas d'une erreur ou d'une faiblesse humaine, comme l'exprime parfaitement ce strip de XKCD sur la sécurité.



Ces limites valent aussi pour le chiffrement des communications.

Pour aller plus loin :

Sur la cryptologie et le chiffrement en général

Plus généralement, le chiffrement des données et des communications ouvre un débat public. En effet, cette protection sérieuse, nécessaire pour sécuriser sa vie privée, ses données et ses communications, peut rendre plus complexe le travail des différentes autorités. Le débat est vif, on peut s'en convaincre avec les articles suivants :

- la page Wikipedia sur le Chiffrement sur le chiffrement avec des rappels historiques,
- P. Aigrain, Blog Mediapart, 5 fév. 2015, *Le droit à l'anonymat et au chiffrement*,
- G. Champeau, Numerama, 8 sept. 2015, *Les eurodéputés demandent le chiffrement systématisé de bout en bout*,
- A. Guiton, Liberation, 13 sept. 2015, *Cryptographie : la justice cherche la clé*,
- S. Bortzmeyer, sur son blog, 1 sept. 2013, *La cryptographie nous protège t-elle vraiment de l'espionnage par la NSA ou la DGSE ?*,
- S. Bortmeyer, sur son blog, 7 nov. 2013, *L'IETF et l'espionnage, et maintenant ?*,
- H. Corrigan-Gibbs, nov.2014, The Intercept (en anglais), *Keeping Secrets*, qui retrace l'historique du conflit politique "chercheurs contre NSA" autour du chiffrement,
- Zythom, expert judiciaire en informatique, zythom.blogspot.fr, *Face à Truecrupt*, qui évoque la protection que permet Truecrypt ainsi que les aspects juridiques et pénaux du chiffrement,
- attention au vocabulaire : le champ disciplinaire s'appelle la "cryptologie". Le chiffrement utilise un code pour rendre un message incompréhensible, le déchiffrement pour le rendre compréhensible à l'aide de la bonne clé. Alors que décrypter signifie "casser le code du message" sans connaitre la clé.
- sur Nonblocking.info, *Cryptographie de comptoir*, quelques éléments présentant le chiffrement et des explications sémantiques sur les termes inadaptés (cryptage, etc.).

Sur le chiffrement de ses données

- La distribution Gnu-Linux Tails - The Anonymous Incognito Live System, compile les principaux outils de protection des données et des communications et peut être utilisée en Live-USB pour garantir au mieux la protection de données sensibles.
- Moserware.com, A Stick Figure Guide to the Advanced Encryption Standard (AES), une BD pédagogique en anglais sur le chiffrement et l'algorithme AES. Elle commence par les notions très simples et elle se termine par des aspects très techniques,
- un article très complet de M. Lee sur *The Intercept* (en anglais), *Encrypting Your Laptop Like You Mean It*, explique ce que permet ou non le chiffrement et les attaques possibles. Toutefois, l'article propose d'utiliser (et décrit comment le faire) BitLocker pour Windows et Filevault pour OS X, deux logiciels que le CECIL déconseille,
- Gfi.com (en anglais), *The top 24 free tools for data encryption*, un résumé des différents outils de chiffrement existants,
- un tutoriel de l'*EFF*, *Instructions de chiffrement de votre dispositif Windows*. Attention, rien ne garantit qu'il n'y ait pas de porte dérobée sur Windows ou OS X donnant un accès insoupçonné aux données déchiffrées,
- À noter que Veracrypt est un *fork* du logiciel libre *TrueCrypt* qui autrefois faisait référence, mais a été victime d'un épisode étrange en 2014. Il s'appuie toutefois sur une ancienne version de TrueCrypt qui a été auditée et ne semble pas contenir de failles de sécurité,
- le logiciel BleachBit (équivalent libre de CCleaner) permet de supprimer définitivement les données en réinscrivant des 0 et des 1 aléatoirement à la place des anciens fichiers en de multiples passages. Il permet aussi de supprimer d'autres traces (fichiers temporaires, historiques de navigation, précédentes recherches...). Un tutoriel d'utilisation présentant aussi ses limites (notamment sur les clés USB et les disques SSD) est disponible sur le site https://ssd.eff.org/fr/. Sur ce point voir également les préconisations du Guide d'autodéfense numérique : Guide.boum.org, Effacer des données "pour de vrai".

Fiche 12. Le chiffrement des communications

Si protéger ses données enregistrées est une bonne pratique, il est tout aussi fondamental de protéger ses communications : courriels, discussions et échanges avec les sites Internet.

12.1 Le chiffrement asymétrique

S'agissant des communications, les méthodes de chiffrement sont différentes de celles présentées précédemment dites "*symétriques*" (le même code est utilisé pour chiffrer et déchiffrer).

En effet, il faut que la personne ou le serveur avec qui l'on communique soit capable aussi bien de déchiffrer les messages qui lui sont envoyés que de chiffrer ceux qu'il envoie pour que la communication ne puisse être comprise par quelqu'un qui "écouterait" le réseau.

Une solution est de partager un code entre les deux correspondant·es (*chiffrement symétrique*), mais cela implique une confiance totale et pose de gros problèmes pratiques (transmission du code, besoin d'autant de codes que de correspondants...). Des solutions plus efficaces permettent de ne pas "partager" son code de déchiffrement tout en chiffrant la communication.

Ce sont les méthodes de chiffrement dites "*asymétriques*". De façon simplifiée, chaque correspondant utilise deux clés : une clé publique communicable à tous, servant à chiffrer les messages, et une clé privée nécessaire pour les déchiffrer.

La clé privée, à ne pas communiquer, est protégée par une phrase de passe personnelle.

Cela peut sembler étrange qu'une clé qui permet de "chiffrer" ne puisse pas permettre de "déchiffrer", mais ces méthodes ont fait leurs preuves.
Une image utilisée est que la clé publique correspond à des cadenas ouverts distribués aux correspondant·es, qui une fois refermés par eux ne peuvent être ouverts que par l·a détent·rice de la clé privée (qui a envoyé les cadenas).

Ces méthodes sont aussi utilisables en tant que "signature" pour authentifier une communication ou un document. On signe le document avec sa clé privée, dont l'authenticité peut être vérifiée à la réception grâce à la clé publique.

12.2 Chiffrer ses navigations

Une des applications de cette méthode est le protocole TLS (pour *Transport Layer Security* couramment utilisé sans en avoir toujours conscience en naviguant sur Internet. C'est le "s" du "HTTPs" ou le petit cadenas vert qui apparait dans la barre d'adresse du navigateur.
Automatiquement, avant toute transmission d'informations, les deux ordinateurs mis en contact (exemple : le votre et celui de votre banque), génèrent puis se transmettent leurs clés publiques et déchiffreront avec les clés privées correspondantes.

Ce petit "s" a donc une importance considérable. Sans cela, un "espion" connecté à un réseau Wifi ou au réseau filaire du quartier ou du noeud réseau, le propriétaire du noeud TOR de sortie de la communication, etc., pourrait connaitre le contenu des échanges (coordonnées bancaires...).

Le module complémentaire "HTTPs Everywhere" de l'*EFF* permet de tester en permanence s'il est possible d'établir une communication en HTTPs et si oui la force.

Pour l'installer sur Firefox :

> Télécharger le logiciel dans la base de modules de Firefox en cliquant sur "Ajouter à Firefox", cliquer sur "Installer", redémarrer le navigateur.

Attention, si l'HTTPs protège la confidentialité du contenu des échanges, mais l'existence d'une communication entre A. et B. et son horaire restent connus. Pour dissimuler ces informations d'autres protections sont nécessaires.

12.3 Chiffrer ses échanges personnels

Une autre application de ce mécanisme de clé privée / clé publique consiste à chiffrer volontairement ses communications personnelles (courriels, messagerie instantanée, SMS et autres communications par ordiphone...).

Pour ce faire, il existe un standard efficace "*OpenPGP*" pour *Pretty Good Privacy* qui est notamment mis en œuvre par un logiciel libre appelé GPG (*Gnu Privacy Guard*).

Même si GPG est moins "automatique" que l'HTTPs, il n'est pas si difficile de chiffrer ses courriels à condition de convaincre ses correspondant·es d'en faire autant.

12.3.1 Chiffrer ses courriels

- Il faut commencer par installer le logiciel GPG, installé par défaut dans la plupart des distributions Gnu-Linux.

> Pour Windows, télécharger et installer (en suivant les consignes) : Gpg4win.
>
> Pour Mac OS X, télécharger et installer (en suivant les consignes) : GPGTools.

Avec Thunderbird

Pour chiffrer ses courriels avec Thunderbird, il suffit de :

> télécharger le module Enigmail. Thunderbird lancé, cliquer sur l'icône des préférences, puis sur "Modules complémentaires", dans la barre de recherche chercher Enigmail et l'installer.
>
> Ensuite, après redémarrage de Thunderbird, dans "Préférences", choisir "Enigmail" -> "Gestion de clé" puis dans la nouvelle fenêtre ouvrir le menu "Générer" -> "Nouvelle paire de clés".
>
> Choisir l'adresse concernée, indiquer une phrase de passe, qui protègera la clé, dans l'onglet avancé choisir une clé RSA 4096 (sur le délai d'expiration voir "pour aller plus loin"). Cliquer sur "Générer la clé".

Ainsi est générée la paire "clé publique / clé privée", la clé privée étant protégée par la phrase de passe.

Cette opération est facile, celle de chiffrer un message également. Ces échanges chiffrés nécessitent toutefois que les autres correspondants disposent aussi d'une paire de clés et que l'on récupère leurs clés publiques.

Pour cela soit on reçoit la clé publique et on l'ouvre le fichier *via* Enigmail, soit il faut la chercher dans un annuaire.

> L'accès à ces annuaires se fait dans la fenêtre "Gestion des clés" d'Enigmail. Cliquer sur "Serveurs de clés" et indiquer l'adresse du correspondant en espérant qu'il ait publié sa clé.

À chaque rédaction de courriel, muni de la clé publique d'un·e correspondant·e, on peut alors chiffrer le message en appuyant sur le cadenas en haut de la fenêtre.

Le même cadenas permet aussi d'authentifier son message par une signature chiffrée.

En utilisant un Webmail

Il est également possible d'utiliser le module Mailvelope sur Firefox (ou Chrome), qui gère l'utilisation de GPG pour les Webmails à partir du navigateur. Cette solution n'est pas la plus conseillée, car le navigateur est un logiciel plus complexe qu'un logiciel dédié à la seule gestion des courriels et a plus de chance de permettre une attaque sur la confidentialité des échanges (par exemple via un autre module).

Cette possibilité fonctionne quel que soit le Webmail, de préférence ceux conseillés par le CECIL, mais même chez les acteurs commerciaux (Gmail, Yahoo, Free, Laposte.net, etc.).

> Il suffit d'ajouter l'extension Mailvelope, alors un petit cadenas avec une clé s'affiche dans la barre de recherche.
>
> Soit l'on dispose d'une paire de clés que l'on peut "importer", soit le module peut en générer comme avec Thunderbird.

Pour chiffrer avec Mailvelope :

> En étant connecté sur son Webmail, l'icône d'un petit bloc-notes avec un crayon apparait dans le corps du courriel. Si l'on possède la clé publique d'un destinataire, en cliquant sur cette icône il est possible de chiffrer le message.

Pour lire un courriel chiffré, il suffit de saisir sa propre phrase de passe.

Ces indications sont sommaires et ont pour seule vocation d'aider à faire les premiers pas. Il est vivement recommandé de consulter des tutoriels plus complets disponibles en fin de fiche pour comprendre les erreurs à ne pas commettre !

À noter en complément à la fiche 8 sur les hébergeurs de courriels alternatifs, le Webmail suisse ProtonMail.ch propose à la fois un chiffrement par défaut entre titulaires de compte Proton Mail, une gestion de PGP plus large, mais aussi un mécanisme de chiffrement à clé unique (transmise par un autre biais) pour transmettre des courriels chiffrés à des correspondants peu motivés à installer un dispositif ou l'autre. Il peut constituer une solution convenable pour chiffrer des échanges courriels.

12.3.2 Chiffrer ses autres échanges

Les discussions sur Internet ne passent pas que par courriels : forums, discussions directes, qu'elles soient audio, vidéo ou textuelles par *tchat*.

Il existe des solutions (utilisables sur les différents systèmes d'exploitation) qui permettent de discuter en ligne de façon plus sécurisée et que le CECIL recommande :

- Jitsi.org, (en remplacement de Skype) qui offre un service protégé pour des échanges audio et/ou de tchat,
- Tox.chat et Ring.cx évoqués fiche 7 offrent des services de conversations audio comme textuels chiffrés,
- Crypto.cat permet de créer des tchats intégralement chiffrés.

Si l'on souhaite absolument continuer à utiliser sa méthode de tchat habituelle (live, gtalk, Facebook...), il reste possible de chiffrer ses communications. Cela nécessite aussi que les correspondants installent un autre logiciel tel que Jitsi ou Pidgin qui acceptent ces méthodes de tchat et auxquels on peut adjoindre le plug-in Off-The-Record (ou OTR) qui va offrir un chiffrement asymétrique avec ses correspondants (selon le même principe d'échanges de clés).

Ces logiciels sont globalement assez simples à prendre en main et intuitifs dans leurs fonctionnements, le plus difficile reste toujours de convaincre ses correspondant·es de les utiliser !

Pour aller plus loin :

Sur le chiffrement des communications en général :

- Framablog.org, *Le chiffrement maintenant*, une traduction par Framasoft d'un guide anglais sur les bonnes pratiques du chiffrement de ses communications,
- un article très complet de M. Lee sur The Intercept (en anglais), *Chatting in Secret While We're All Being Watched*, expliquant comment protéger autant que possible ses communications en alliant TOR et le chiffrement.

Sur l'HTTPs :

- Wiki.linuxwall.info, *Principes du chiffrement avec le protocole SSL/TLS*,
- sur le site de l'EFF, la FAQ de l'extension HTTPs Everywhere (en anglais) qui permet de comprendre de nombreux aspects du fonctionnement de l'extension et du protocole.

Sur GPG - PGP et chiffrer ses courriels :

Pour compléter les indications de cette fiche et chiffrer correctement ses messages :

- une explication des bonnes pratiques sur GPG sur le site RiseUp.net, *Open PGP Best practices*,
- autodéfense courriel, un tutoriel de la Free Software Fondation (en français) pour chiffrer ses courriels
- PGP sous Windows/Linux/Mac Le b.a-ba celui de l'EFF aussi en français.
- le tutoriel d'OpenPGP, openpgp.vie-privee.org et sur securityinabox.org (en anglais) un guide pour Enigmail sous Thunderbird,
- S. Bortzmeyer, sur son blog, *Ma nouvelle clé PGP*, quelques indications pour créer une clé GPG fiable,
- un tutoriel sur Mailvelope sur le site Openclassrooms.com, **Utilisez GPG depuis votre webmail grâce à Mailvelope**
- depuis les révélations d'E. Snowden, les différents logiciels présentés dans cette fiche ont des communautés actives visant à les améliorer et en démocratiser l'usage. GPG ou Enigmail sont constamment en train d'être améliorés.

Fiche 13. Les ordiphones

Des ordinateurs de poches accompagnent une grande majorité d'entre nous. Ces ordiphones (ou *smartphones*) sont devenus des interfaces pour de nombreux usages du quotidien. Pourtant, ces couteaux suisses numériques constituent souvent une faille importante pour la sécurisation des données et la protection des libertés. Conçus pour communiquer, ils intègrent de nombreux capteurs chargés, en permanence, d'analyser (et de quantifier) l'environnement de l'appareil : détection et connexion à de nombreux réseaux, capteurs visuels (photo et vidéo), microphone, géolocalisation, position spatiale (accéléromètre), etc.
Ces petits ordinateurs sont plus difficilement contrôlables que leurs ainés : ils sont rarement "non connectés", les composants sont souvent plus spécifiques et les constructeurs exercent un pouvoir plus élevé sur ces matériels. La contrainte la plus conséquente vient des fournisseurs du système d'exploitation. Il s'agit d'un secteur duopolistique où Google et Apple sont très largement majoritaires et imposent, par défaut, un compte connecté chez eux pour utiliser l'appareil ainsi que des logiciels de bases souvent impossibles à supprimer. Cette dépendance à ces deux acteurs dont les atteintes aux libertés sont fréquemment dénoncées pose problème et il est difficile de trouver ou mettre en place des alternatives éthiques. Il faut donc acter qu'il existe un problème intrinsèque des ordiphones en matière de respect des libertés.
Des méthodes simples permettent néanmoins de limiter les dégâts face à d'autres atteintes possibles. Comme pour un ordinateur classique, il existe des applications et des bonnes pratiques permettant de mieux protéger ses données : utiliser des phrases de passe, chiffrer ses données et ses communications, se renseigner sur les services que l'on utilise et opter pour des services respectueux des libertés, utiliser des applications libres, etc. De plus, des projets d'ordiphones "libérés" et systèmes d'exploitation plus éthiques se développent.

13.1 Quelques bonnes pratiques de paramétrage

Les ordiphones peuvent facilement être volés, perdus ou victimes d'applications malveillantes. Adopter de bonnes pratiques, activer des paramètres de sécurité et chiffrer ses données vont assurer une première couche de protection.

- Minimiser les données stockées : face à la vulnérabilité de tels appareils, mieux vaut limiter les données qui y sont stockées et ne pas y conserver de données sensibles telles que des coordonnées bancaires, des mots de passe, des codes d'accès, des informations médicales, etc.
- Activer le code PIN : il sera demandé à chaque allumage et constitue une mesure basique. Il ne protège que l'accès aux réseaux de communication de l'opérateur *via* la carte SIM. Attention : sans autre mesure de protection, les données de l'appareil resteront accessibles et celui-ci pourra toujours être connecté en Wifi. Il est également important de remplacer le code par défaut (0000, 1234…)
- Conserver son code IMEI : c'est le numéro de série de chaque ordiphone. En cas de vol, il permet de bloquer l'usage du téléphone sur tous les réseaux. Il est possible de l'obtenir en tapant *#06# sur le clavier du téléphone.
- Verrouillage de l'appareil : à chaque extinction de l'écran, un code d'accès est demandé pour déverrouiller l'ordiphone. Il s'agit de sécuriser l'accès rapide à l'appareil. Sans ce code, impossible d'utiliser directement l'ordiphone, couplé au chiffrement des données cela limite grandement les accès aux données en cas d'accès illégitime à l'appareil. Le verrouillage s'active facilement dans les paramètres de sécurité. Il est préférable de privilégier un code plutôt qu'un schéma, facile à observer, ou des données biométriques.
- Maitriser ses capteurs : les ordiphones disposent de nombreux capteurs. Il est possible d'en rendre certains inactifs en les paramétrant. Il est ainsi conseillé de les désactiver dès qu'ils ne sont plus utilisés. Il s'agit surtout de la localisation GPS qui peut être utilisée et récupérée par de nombreuses applications même en apparence inactives, mais aussi de la connexion Bluetooth, ou même Wifi et réseaux mobiles (qui permettent potentiellement de tracer les positions et les lieux visités). Dans les périodes où la connexion n'est pas nécessaire, il ne faut pas hésiter à passer son téléphone en mode « avion » pour limiter les données de connexions. Il est important de désactiver ces connexions dès qu'elles ne sont plus nécessaires et de minimiser la production de données exploitables. Cela ne doit toutefois pas faire oublier l'impossibilité d'un contrôle complet par l'individu : les ordiphones peuvent être utilisés comme des mouchards de poche.

- **Vérifier et maitriser ses paramétrages** : si par défaut un grand nombre d'informations sont transmises aux entreprises « présentes » sur les appareils (Apple, Google, constructeurs, applications…), certains paramétrages permettent de limiter cela. Il est possible de désactiver les « statistiques d'utilisation », mais aussi la fonction « Ok Google ».

  > Cette fonction est cachée dans les paramètres, langue et saisie, Saisie Vocale, reconn. Google de Base, roue paramètre, Détecter « Ok Google » et tout désactiver.

D'autres paramétrages peuvent s'avérer pertinents : créer un compte invité, indiquer un contact sur son écran de « verrouillage » dans le cas où l'ordiphone serait perdu et pourrait être retourné, etc. Il est vivement conseillé de prendre le temps de les explorer pour mieux maitriser son appareil.

- **Chiffrer les données stockées** : sur les versions les plus récentes des systèmes d'exploitation mobiles, cette option est simple à activer et ne demande aucune compétence particulière.

  > Sur Android, il suffit d'aller dans les paramètres. Puis « sécurité » et d'appuyer sur « chiffrer le téléphone ». L'opération est irréversible et demande un peu de temps. À chaque démarrage, le code sera demandé pour déchiffrer l'appareil ainsi qu'au déverrouillage si l'option est activée.
  >
  > Sur iOS, le chiffrement est désormais activé par défaut et il suffit de configurer un mot de passe, dans « Paramètres généraux » et sélectionner « Mot de Passe » ou « Code d'Accès… » pour activer la protection.

- **Contrôler les autorisations de ses applications** : sur les versions les plus récentes des systèmes d'exploitation mobiles, il est possible de contrôler les permissions des différentes applications présentes sur son téléphone et de désactiver celles qui sembleraient problématiques.

  > Sur Android 6.0 et +, il faut aller dans « Paramètres », « Applications », cliquer sur la roue dentée puis sur « Autoris. des applis ».
  > Sur iOS, le système est différent. Pour activer certaines permissions un accord est demandé, il reste possible ensuite de consulter les applications séparément pour désactiver les permissions jugées non pertinentes ou de consulter globalement celles-ci en allant dans « Paramètres », « Vie privée ».

À noter que pour Android, l'association « Exodus Privacy », Exodus-privacy.eu.org offre une analyse des permissions demandées par les différentes applications ainsi que des empreintes des traqueurs contenus dans ces applications révélant l'ampleur de la surveillance sur ces applications.
Une application « Exodus Privacy » pour mobile devrait voir le jour, mais le site Internet constitue déjà un formidable outil pour découvrir ces traqueurs et faire le tri dans ses applications.

13.2 Des applications libres plus respectueuses des libertés

Sur ordiphone, toutes les applications ne se valent pas et les conseils précédemment donnés continuent de s'appliquer : privilégier des applications libres et éthiques et limiter le nombre d'entre elles au strict nécessaire. Malgré les incitations à installer des applications dédiées, il est souvent préférable de se contenter de la page Web mobile du service souhaité pour limiter les traqueurs et l'usage des ressources de l'appareil.

13.2.1 F-Droid

Sur les systèmes types « Android », il existe une application regroupant les applications libres : F-Droid. C'est l'équivalent d'un « magasin d'applications » qui répertorie les applications libres et facilite leurs installations et mises à jour.

Pour l'installer :

> Sur le navigateur de son ordiphone, se rendre sur le site de « F-Droid », https://f-droid.org et cliquer sur « Télécharger F-Droid », cela récupèrera l'APK (fichier exécutable de l'application permettant de l'installer) qui devra être lancé pour installer F-Droid. Il faudra peut-être pour cela accepter les « applications provenant de sources inconnues ».

Une fois installé, F-Droid vous permettra d'accéder facilement à certaines des applications citées ici et de les installer et mettre à jour. Attention, d'autres ne seront présentes que sur Google Play (ou directement en APK sur Internet). Les concepteurs de F-Droid sont assez exigeants sur les engagements sur le logiciel libre et l'absence de traqueurs, des exceptions sont tolérées selon les cas, mais toujours mentionnées en tant « qu'antifonctionnalités » (publicités, recours à des éléments annexes non libres…) et il est préférable de bien lire la fiche de chaque application.
Par exemple, pour installer « Silence » (application conseillée plus loin) :

> Lancer F-Droid, Appuyer sur la loupe, Taper « Silence » puis cliquer sur installer à côté de Silence.

Il n'existe pas pour le moment d'équivalent sur iOS, où certaines applications demeurent néanmoins libres (il en va de même sur Google Play).

13.2.2 Les applications de base

Une fois cela fait, les conseils applicables aux ordinateurs s'appliquent à nouveau :

- Installer Firefox en remplacement du navigateur par défaut. Pour cela, il suffit d'aller sur Google Play ou l'AppStore d'Apple et de l'installer Firefox. Il est ensuite possible de l'utiliser par défaut et d'y adjoindre les modules de protection souhaités (notamment uBlock Origin et Decentraleyes) en passant par l'ajout de modules complémentaires au sein de Firefox.
- Il existe également « Firefox Klar ou Focus » conçu pour réaliser des navigations uniques et va isoler la plupart des informations pour limiter le traçage.
- On peut alors changer de moteur de recherche (Qwant, Startpage, Searx…) en allant sur la page du moteur de recherche souhaité et en restant appuyant longuement sur le champ de recherche pour l'ajouter puis le sélectionner par défaut dans les paramètres de recherche.

Le CECIL recommande par ailleurs quelques applications pour des usages fréquents sur mobile :

- **OsmAnd~** disponible sur F-Droid, qui offre un service de localisation et navigation GPS s'appuyant sur les cartes libres d'OpenStreetMap. Il faudra ensuite télécharger les cartes pertinentes à partir de l'interface de l'application (qui resteront accessibles même sans réseau) ;
- **K-9 Mail**, comme application de gestion de courriel pour ordiphone qui permet d'ajouter et de gérer ses comptes. Il faut également noter que Protonmail dispose d'une application dédiée.
- **Twidere** pour utiliser des comptes Mastodon et Twitter ;
- **Nextcloud** pour synchroniser des données en ligne sur un serveur de confiance (par exemple celui de La Mère Zaclys ainsi que DAVDroid qui est un outil de synchronisation de ses contacts et de son agenda complémentaire à une solution Nextcloud ;

- Il est également possible d'utiliser le réseau TOR sur Android par la combinaison de deux applications développées par le Guardian Project : **Orbot** et **Orfox** disponible sur F-Droid. Sur iOS, il existe aussi une application qui n'est toutefois pas officiellement reconnue par le Projet TOR et qui présente certaines limitations imposées par Apple : « Onion Browser ».

13.3 Des applications de chiffrement de bout en bout des communications

Comme pour Internet, les téléphones ont été principalement conçus pour faciliter les communications, les problématiques de sécurisation et de protection des correspondances ne sont venues qu'ensuite. De ce fait, les communications échangées classiquement par téléphone peuvent potentiellement être interceptées (selon les cas plus ou moins facilement) ou récupérées par les opérateurs ou les services de renseignement.
Pour remédier à ce problème, des applications ont été développées pour retrouver une certaine protection de ses communications en ligne.

Il n'existe pas de solution parfaitement libre, décentralisée, fonctionnelle, multiplateforme, interopérable, sans aucun défaut éthique, etc. Le CECIL recommande toutefois deux solutions qui permettent de facilement améliorer la sécurité de ses communications en mettant en place un chiffrement de bout-en-bout géré automatiquement par l'appareil et protégeant donc le contenu des échanges sur le réseau.

13.3.1 Signal, pour chiffrer ses appels et ses messages textes

Signal est une application disponible sur iOS et Android qui permet de chiffrer de bout-en-bout et par défaut les communications qui transitent par l'application. Elle assure alors la protection des discussions téléphoniques ou textuelles. Ce logiciel libre est développé par la société Open Whisper Systems qui est principalement financée par des subventions et des dons. Elle a mis en place un protocole de chiffrement des communications par Internet mis en œuvre dans l'application Signal.
L'application est gratuite et s'installe facilement. C'est une application de messagerie texte très commune en apparence où le chiffrement est géré sur l'ordiphone de la personne sans aucune complexité. L'application dispose même d'une interface pour ordinateur qui impose toutefois d'avoir Chrome (le navigateur de Google).
Une autre limite à cette application est qu'elle doit être liée à un numéro de téléphone dont on doit garder le contrôle et qui sera publiquement diffusé. C'est pour le moment justifié par la nécessité de savoir lesquels de ses contacts utilisent également Signal pour échanger avec eux de façon chiffrée. Signal refuse par ailleurs de permettre une interopérabilité avec d'autres clients de messagerie.

13.3.2 Silence, pour chiffrer ses SMS

Silence est une application libre de chiffrement issue d'un fork du logiciel TextSecure disponible uniquement pour OS type Android.
Silence permet d'échanger des SMS chiffrés sans requérir de réseau Internet. Il ne requiert pas non plus de devoir déclarer son numéro.

> Une fois installé, il suffit de réaliser un échange de clés (conservées sur l'appareil) par un simple clic sur une icône de cadenas ouvert au sein d'une discussion avec une autre personne disposant de Silence.

L'application permet aussi d'échanger des SMS non chiffrés avec les personnes ne disposant pas de Silence et peut être utilisée comme application SMS par défaut.

Pour ces deux applications, il est recommandé d'activer le verrouillage de l'application et le chiffrement de ses données par une phrase de passe. Cela empêchera toute personne qui obtiendrait votre téléphone déchiffré d'accéder à vos communications sans ce code.

Pour cela, aller dans Paramètres, Vie privée, Activer le verrouillage et entrer un code.

D'autres applications libres proposent la protection des communications par du chiffrement bout-en-bout, par exemple, Riot.im, Wire ainsi que le projet Briar, mais restent, pour le moment, plus marginales en nombre d'utilisateurs.

Le CECIL déconseille par ailleurs l'usage de Telegram qui malgré sa relative notoriété et une solution de chiffrement des échanges activable n'est pas libre aussi bien en ce qui concerne l'application que sur les méthodes de chiffrement. Son algorithme de chiffrement n'est donc pas auditable et sa sécurité est loin d'être prouvée. De plus, l'application ne propose pas le chiffrement par défaut des conversations, malgré la croyance, ni celui des conversations en groupe. Le CECIL déconseille également l'usage de WhatsApp qui s'appuie pourtant sur le protocole de chiffrement de Signal, mais qui est détenu par Facebook qui a tout fait pour exploiter les numéros de téléphone des personnes utilisant WhatsApp avec les données de Facebook et certaines métadonnées.

13.4 Des systèmes d'exploitation libres : Lineage OS

Android, le système d'exploitation de Google a été construit sur la base de logiciels libres et son noyau est donc libre et théoriquement librement réutilisable. Google a toutefois su parfaitement exploiter les avantages de « l'*open source* » (contributions volontaires bénévoles, reprises d'éléments de code existant…) tout en essayant de bloquer toutes les formes de concurrence par des partenariats agressifs avec les constructeurs imposant l'installation des « Google Mobile Services » (GMS) par défaut et en interdisant le recours à des dérivés ("*forks*") d'Android. Google contrôle également l'accès au « Google Play Store » qui s'est par ailleurs imposé comme un accès quasi-nécessaire à de nombreuses applications et a d'autres pratiques similaires. À l'exception des iPhone, le système d'exploitation Android monopolise désormais le marché.

Face à cette situation de nombreux projets ont vu le jour pour mettre en place un système d'exploitation pour ordiphone fiable et libéré de Google, mais la tâche est ardue et beaucoup ont été abandonnés face à ces contraintes. Il existe toutefois des projets qui tiennent bon et permettent dans certains cas de libérer son ordiphone de la mainmise de Google et des GMS. La solution la plus répandue et que le CECIL recommande est Lineage OS.

Fork du projet « Cyanogen » s'appuyant sur les éléments libres d'Android, Lineage constitue pour le moment l'alternative la plus simple pour « dégoogliser » un ordiphone sous Android.
Reste que le remplacement de son système d'exploitation sur ordiphone n'est pas aussi aisé que de remplacer Windows sur un ordinateur fixe. Il est nécessaire tout d'abord de pouvoir obtenir les droits administrateurs (dits *root*) sur son appareil, ce qui n'est pas toujours évident ainsi que de disposer d'un « portage » de Lineage spécifique à son appareil, les composants et interactions des différents modèles étant susceptibles de varier grandement.

Ainsi, si sur certains téléphones très achetés et bien documentés (cela peut constituer un éventuel critère de choix dans l'acquisition d'un appareil), le remplacement d'Android par Lineage peut s'avérer relativement aisé pour une personne suivant strictement les instructions et un peu débrouillarde, pour d'autres la tâche peut s'avérer complexe. Une telle opération est par ailleurs susceptible de compliquer une mise en œuvre de la garantie.

Pour qui souhaiterait sauter le pas, en plus de devoir se documenter sérieusement, il existe quelques personnes très motivées et prêtes à aider pour réaliser ce passage. Pour les rencontrer, de bons points d'entrée sont les forums spécialisés ainsi que les « fêtes d'installations » du monde du libre.

13.5 Des appareils plus éthiques à soutenir

Les ordinateurs de poche ne posent pas seulement des problèmes en termes de sécurité et de respect des libertés, les questions de réparabilité et de couts écologiques, mais aussi de provenance des minéraux pour les fabriquer (problématique des « terres rares » provenant de zone de conflits et d'exploitation des mines où travaillent parfois des enfants), l'exploitation d'ouvrièr·es dans la fabrication, etc. posent d'importants enjeux de société.
Une alternative viable sur ces questions est portée par Fairphone. Cette entreprise Néerlandaise a été fondée en 2013 avec pour objectif de concevoir un ordiphone plus respectueux de l'environnement et d'améliorer les conditions productions, de travail et d'extraction :
* pas d'approvisionnement dans les zones de guerre ou permettant le travail des enfants,
* logique de commerce équitable,
* amélioration des conditions de travail,
* objectif de réparabilité maximale,
* recyclage des déchets électroniques.

Difficile d'être parfait en la matière et face aux contraintes économiques Fairphone a dû par exemple arrêter la fourniture des pièces détachées pour le « Fairphone 1 » limitant de fait sa réparabilité et la durée de vie de cette première mouture. Le prix du Fairphone 2 désormais distribué reste élevé (> 500€). Fourni par défaut avec Android, il est par contre facile de le remplacer par « Fairphone Open » qui est un portage de Lineage pour le Fairphone.
Malgré quelques défauts, Fairphone a le mérite d'exister et de rechercher une certaine éthique sur des sujets facilement négligés face à des mobiles moins chers (au prix des conditions de travail à Shenzen et d'approvisionnement sanglant de certains matériaux) ou des approches marketing plus soignées. Les enjeux sont pourtant de taille en termes de droits humains et justifient de soutenir cette initiative.

On peut enfin signaler que bien que son usage se soit imposé socialement, la place et l'intérêt des ordiphones méritent d'être questionnés, la meilleure solution pour limiter ses problématiques restant encore de ne pas en acquérir.

Maxime Lehmann stagiaire au CECIL a participé à l'élaboration de cette fiche.

Pour aller plus loin

Des guides généraux sur la sécurisation des ordiphones et le paramétrage

- Gee, sur son blog Grisebouille.net, "Fairphone un téléphone pour libriste", qui détaille ses étapes pour "dégoogliser" au mieux son ordiphone et ses applications ;
- Sur le site de la Cnil.fr, "Maitriser les réglages vie privée de votre smartphone", 5 janv. 2015 et "Comment sécuriser au maximum l'accès à votre smartphone ?", 27 janv. 2017 ;
- Les guides de l'EFF, "Guides sur les outils" ;
- Anssi, ssi.gouv.fr, "recommandations de sécurité relatives aux ordiphones" ;
- Guide de l'association Nothing 2 Hide, "Protégez vos anonymats sur téléphone portable" ;
- A. Hern, TheGuardian.com, "Your battery status is being used to track you online" (en anglais) ;
- Freedom of the presse foundation, "Mobile security prevention tips" (en anglais).

Sur les applications libres et la sécurisation

En plus des applications citées, il est pertinent de se renseigner sur :
* AFWall +, qui permet sur un ordiphone "rooté" de bloquer l'accès à Internet d'application qui n'en ont pas besoin ;
* Haven, développée par le Guardian Project en collaboration avec E. Snowden qui permet d'utiliser les capteurs de l'ordiphone à des fins de sécurisation face à des atteintes extérieures illégitimes.

Sur la question du chiffrement sur ordiphone

- Voir les autres travaux du Guardian Project sur leur site Guardianproject.info ;
- M. Shelton, sur Medium.com, Signal for begginers", 18 nov. 2016 (en anglais) ;
- Sur la critique de Telegram, The Grugq sur Medium.com, "Operatinal Telegram", 18 nov. 2015 (en anglais) ;
- Il est possible de faire fonctionner PGP sur son ordiphone via K9-Mail en utilisant OpenKeychain, voir le tutoriel "Open Keychain Usage" sur le site k9mail.github.io ;
- Il est aussi possible d'utiliser un client XMPP et "Off The Record" sur ordiphone par exemple avec Xabber ou Conversations ;
- Il faut relever que le chiffrement des ordiphones fait l'objet de vifs débats publics et est très attaqué comme dans le cas de l'affaire "FBI vs Apple". En France, le fait de refuser de déchiffrer son appareil sur demande d'une autorité judiciaire peut potentiellement être sanctionné en tant que tel.

Sur les systèmes libres

- Le site Internet Lineageos.org ;
- On peut aussi découvrir différents projets essayant de porter un système d'exploitation libre pour ordiphone : UBPorts, Sailfish OS, Replicant, LuneOS, QubeOS Librem et le récent Eelo qui bénéficie d'un financement participatif réussi.

Enfin, pour questionner la place de l'ordiphone dans sa vie, Lapalice.fr, "Sans smartphone point de salut", le 21 fév. 2018.

Fiche 14. Pour continuer l'aventure...

Ces petites fiches constituent un premier pas pour retrouver un peu d'intimité et de liberté dans le monde numérique. Il s'agit de reconquérir un certain contrôle sur ses données et une certaine autodétermination informationnelle.

Il ne s'agit toutefois que de préconisations générales qui peuvent ne pas correspondre à des cas particuliers. La sécurité est un processus, pas un produit, ces premiers pas permettent de se lancer dans ce processus. Pour aller plus loin et découvrir d'autres approches, le CECIL recommande de découvrir :

- Le guide d'autodéfense numérique, éd. Tahin Party disponible en version papier à 15€ ou sur Guide.boum.org;
- Les préconisations de l'Electronic Frontier Foundation sur le site Ssd.eff.org/fr;
- Le site Prism-break.org, qui propose des outils alternatifs libres, décentralisés et respectueux des libertés;
- La distribution Gnu-Linux TAILS : "The Anonymous Incognito Live System", conçue pour protéger aux mieux ses données dans ses pratiques numériques : Tails.boum.org;
- Contrôle tes données, le site d'information sur le sujet de La Quadrature du Net : Controle-tes-donnes.net;
- "Autodéfense courriel", un tutoriel poussé de la Free Software Foundation sur le chiffrement des courriels, Emailsselfdefense.fsf.org/fr/.
- Libre et humain à l'ère d'Internet, d'A. Delalain et H. Pierre, un petit ouvrage pour comprendre pourquoi et comment protéger sa vie privée sur Internet, livre numérique à 5€.

Il ne faut toutefois pas oublier que si l'autodéfense numérique est importante, elle est insuffisante face aux possibilités des Etats et des grandes entreprises du numérique. Pour contrôler leurs pouvoirs et pousser vers de meilleurs équilibres, le combat politique est nécessaire. Pour cela il est important de soutenir des associations qui agissent au quotidien sur ces questions :
* L'Observatoire des Libertés et du Numérique et ses associations membres : Amnesty International France, Le CECIL, Creis-Terminal, La Ligue des Droits de l'Homme (LDH), La Quadrature du Net (LQDN), Le Syndicat des Avocats de France (SAF), Le Syndicat de la Magistrature (SM);
* Les associations défendant le logiciel libre et ses libertés telles que Framasoft, l'April et les nombreuses associations et CHATONS locaux;
* Les fournisseurs d'accès associatifs de la Fédération "French Data Network";
* Le collectif "Café vie privée";
* L'association "Nos Oignons";
* Et à l'échelle internationale des associations telles que Privacy International, Edri "European digital rights" et l'Electronic Frontier Foundation.