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

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 de citoyens (majoritairement non américains) souvent par l'intermédiaire de compagnies telles que Microsoft, Yahoo, Google, Facebook, AOL, Apple… En plus de cette surveillance étatique, un utilisateur 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 au citoyen inquiet, quoique peu connaisseur, 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 qu'Ubuntu pour le système d'exploitation ou Firefox pour le navigateur.

2. Les logiciels libres

Face aux grands éditeurs dits "propriétaires" (Microsoft, Apple, Adobe…), depuis plus de trente ans, nombreux sont 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 à l'utilisateur 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 maîtrise de nos outils est un enjeu majeur. Ce combat est aussi mené par les défenseurs du logiciel libre.

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 utilisateurs 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 de leurs utilisateurs. C'est par exemple le cas de Qwant, DuckDuckGo ou d'IxQuick.

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 utilisateurs 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 Disconnect, 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 nombreux utilisateurs 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 coût indirect, car ils tracent une partie importante des activités des utilisateurs 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.

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 TOR et les réseaux privés virtuels.

11-12. Le chiffrement

Le stockage et la transmission d'une partie de plus en plus conséquente 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 par le biais d'une faille informatique ou d'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 indûment connaissance.

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

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

1. 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, le consommateur 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 (smartphones), qui comme le nom français l'indique sont en réalité bien plus des ordinateurs, capables aussi de téléphoner. 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 coût 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 utilisateurs : 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 d'Ubuntu, de Linux Mint, de Debian ou de Fedora. Une autre 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 ravis d'aider lors d'événements 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 (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 utilisateurs 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 d'utilisateurs n'ont pas été incités à faire de choix.

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 utilisateurs…

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 des utilisateurs (*Encrypted Media Extensions*). Malgré ces concessions, ce navigateur reste un excellent choix qui s'engage véritablement, et de plus en plus, dans la protection de la liberté et de la vie privée de ses utilisateurs.

Les utilisateurs les plus engagés préféreront peut-être d'autres navigateurs libres et sans concessions, tels que Palemoon, Midori ou IceCat, similaires à Firefox (quoique moins développés), mais sans compromission face aux mesures techniques de protection. IceCat intègre de surcroît des modules protecteurs pour la vie privée. Vous pestez contre la surveillance de masse et utilisez encore Internet Explorer ! 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.

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 *a 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'utilisateur. 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,
- un article de NextInpact, *La justice européenne se penchera sur la vente liée PC et OS*.

2. Les logiciels libres

Les systèmes d'exploitation Gnu-Linux comme les navigateurs Firefox ou IceCat présentés Fiche 1 sont tous des "logiciels libres". Ce choix est loin d'être anodin. Ces logiciels libres participent à garantir le contrôle des utilisateurs 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 de ses citoyens. 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 est illisible par l'humain, pour être exécutable par la machine. C'est ce seul code binaire qui est transmis par les éditeurs propriétaires. Ce processus rend impossible, aussi bien pour un utilisateur de base que pour un développeur aguerri, de connaitre le fonctionnement exact du logiciel, ses fonctionnalités et encore moins de le modifier. Sans accès au code source, l'utilisateur 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 :

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

Lorsque l'on qualifie un logiciel comme "libre", on fait ainsi référence aux libertés de ses utilisateurs, 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 ambiguïté 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 ou la licence française CECILL (pour CEa Cnrs Inria Logiciel Libre). C'est par exemple le cas de Firefox pour le navigateur Web, mais aussi de Libre Office 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 développeurs 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 ou Sourceforge), 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 à chacun d'auditer ses logiciels libres et de vérifier qu'il n'y a pas de dissimulation de fonctionnalités cachées ou de portes dérobées (*backdoor*). Pour l'utilisateur de base, 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, 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'Adblock Plus dont le code a été repris, notamment, par uBlock Origin). 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 développeurs. 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 utilisateurs 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 coûts 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 développeurs libres indépendants.

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'utilisateur 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 utilisateurs peut aussi se traduire sous forme de dons pour participer aux développements de logiciels qui bénéficieront à tous. Les développeurs et les utilisateurs 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 événements liés à l'informatique libre. Des "install-party" visant à aider

les particuliers à faire le grand saut et à installer une distribution Gnu-Linux sur leur ordinateur, mais également des événements de grande importance comme l'Open World Forum, qui se réunit annuellement à Paris 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).

3. Les moteurs de recherche alternatifs

Outil central de nos pratiques sur Internet, un moteur de recherche permet de lancer une recherche sur un sujet, un auteur, 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 utilisateurs. Ainsi, chaque recherche lancée s'accompagne d'une collecte discrète de données concernant les préférences de l'utilisateur 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 Qwant, Ixquick ou DuckDuckGo. Il s'agit ici de les mettre en valeur pour inciter les citoyens soucieux de leur vie privée à changer leurs pratiques.

3.1 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 utilisateurs. Le site n'enregistre pas les requêtes et affiche une opposition ferme au traçage. Il utilise son propre moteur de recherche et y ajoute des résultats issus d'autres sources d'informations ouvertes pour enrichir 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.

3.1.1 Les avantages d'utilisation de DuckDuckGo :

- **Confidentialité :** il ne stocke pas d'informations personnelles concernant les utilisateurs, pas même leurs adresses IP (adresse d'identification des ordinateurs sur Internet). La politique défendue est "Don't track us" c'est-à-dire "Ne nous tracez pas". Il offre de nombreuses garanties contre le traçage et conserve le minimum de données possibles sur ses utilisateurs et aucune directement identifiante.
- **Multilingue :** l'interface existe en français et l'essentiel des pages et des fonctionnalités sont désormais également traduites.
- **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 :** 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. Point notable, on peut même accéder à Google sans être tracé (*"!g la requête"*).

- **Engagements citoyens :** une partie des revenus de DuckDuckGo sont de plus consacrés à des projets de développement de logiciels libres protecteurs de la vie privée.

3.1.2 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).

3.2 Ixquick : un métamoteur protecteur européen

Depuis 2006, le moteur de recherche Ixquick prône comme politique le respect intégral de la vie privée de l'internaute et de ses informations personnelles. Contrairement à DuckDuckGo installé aux Etats-Unis, donc soumis à la législation américaine (Patriot Act…), Ixquick est basé aux Pays-Bas. Il est donc soumis à la législation européenne et peut se vanter de travailler avec la CNIL néerlandaise. Il s'agit d'un métamoteur de recherche, c'est-à-dire qu'il ne dispose pas de son propre algorithme d'indexation et de recherche, mais s'appuie sur ceux de Google, Yahoo, etc. Il agrège leurs résultats pour ensuite proposer un résultat adapté à l'utilisateur. Contrairement à eux, il s'engage toutefois sur de nombreux aspects relatifs à la protection de la vie privée sur Internet.

> Pour ajouter Ixquick au navigateur, rien de plus simple, il suffit d'ouvrir la partie téléchargement sur son site et de cliquer sur "Installer" (la version HTTPS de préférence). La procédure détaillée pour DuckDuckGo fonctionne également.

3.2.1 Les avantages d'utilisation d'Ixquick :

- 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,
- la connexion peut être sécurisée en utilisant le protocole de communication chiffrée (HTTPs).
- localisation de la société en Europe, aux Pays-Bas.

On bénéficie ainsi des résultats des principaux moteurs de recherche sans pour autant leurs livrer ses données personnelles. En pratique, Ixquick réalise les requêtes à la place de l'utilisateur. Ce moteur de recherche bénéficie de quelques garanties sur ses engagements. Il a obtenu le label européen pour la protection des informations personnelles et est engagé auprès de l'équivalente néerlandaise de la CNIL.

3.2.2 Des limites :

Néanmoins, la société Surfboard Holding, éditrice d'Ixquick, 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.).

3.3 Qwant : un projet français en développement

Si à son lancement en 2013 le projet était peu convainquant, 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 utilisateurs 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.*"

Les grands atouts de DuckDuckGo ou d'IxQuick sont aussi présents : absence de traçage, cookies limités aux stricts besoins de la recherche, absence de personnalisation des résultats, HTTPs… Il s'agit donc d'une alternative efficace pour protéger sa vie privée. La société Qwant a le mérite d'être située en France 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. L'interface est fluide, fonctionnelle et facile à adopter.

Son financement repose pour le moment sur les achats réalisés *via* son interface de "Shopping" sans causer donc de réels soucis relatifs à la vie privée.

À noter également l'existence d'un moteur de recherche à destination des plus jeunes, respectant autant leur vie privée que les protégeant d'accéder à des contenus peu adaptés : Qwantjunior.

Sans être parfaits, Qwant, Ixquick et DuckDuckGo 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 :

Cette fiche se concentre sur les moteurs ayant une volonté éthique, protectrice de la vie privée et des libertés de leurs utilisateurs. Il existe également Exalead.com, ou encore WolframAlpha.com, intéressants à d'autres égards, sans toutefois avoir le même engagement éthique.

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 DuckDuckGo :

- Softonic.fr, *DuckDuckGo moteur de recherche anonyme oubliez Google*,
- Netpublic.fr, *Apprendre à utiliser DuckDuckGo, moteur de recherche qui respecte la vie privée : 6 tutoriels*,
- le site de DuckDuckGo, Donttrack.us.

Des articles et compléments sur Qwant :

- J. Lausson, Numerama.com, *Eric Léandri (Qwant) : les internautes "doivent-ils désormais se méfier de l'Etat ?"*,
- Korben.info, *Qwant – Mon retour après 1 mois de test*,
- D. Cuny, Rue89, *Qwant, le "Google français" ? On ne ricane pas, s'il vous plaît*.

Depuis les dernières versions de Firefox, il n'est plus possible de changer le moteur par défaut directement dans la barre de recherche.

> Pour rétablir cette possibilité, il faut réaliser une petite modification des paramètres de Firefox : Inscrire "about:config" dans la barre d'adresse puis valider. Valider que "Je ferai attention, promis !". Ensuite réaliser un clic droit n'importe où, puis cliquer sur "Nouvelle" -> "Valeur booléenne". Indiquer "browser.search.showOneOffButtons". Par défaut la valeur devrait être "false". Valider et redémarrer Firefox.

4. L'historique de navigation et les cookies

4.1 Présentation

Internet Explorer, 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 visités par l'utilisateur.

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'utilisateur (données de formulaire, données d'identification à des sites Internet 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'utilisateur. 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 sans laisser de 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. Ces outils sont généralement accessibles via la barre d'outils.

> 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 "Fenêtre privée" dans les options.

Il faut d'ailleurs noter que depuis la version 42, 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, cliquer sur "Historique", puis "Effacer l'historique". 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 protégera 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 FAI (Fournisseur 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).

5. 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 le dit "si c'est gratuit, c'est vous le produit". De nombreux sites vendent donc le "temps de cerveau disponible" de leurs utilisateurs reportant les coûts sur l'achat des produits ou services de l'annonceur. Au-delà du débat sur le bien-fondé de la publicité, celle-ci conduit souvent sur Internet au traçage de données personnelles. Ce traçage peut aller jusqu'au profilage détaillé des utilisateurs, qui peut s'avérer extrêmement dangereux en termes de risques 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.

Les citoyens 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.

Une option présente dans les navigateurs vise à signifier aux sites visités que l'on ne souhaite pas être tracé, le "*Do Not Track*" (ne pas tracer). Le CECIL conseille de l'utiliser, sur Firefox :

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

Malheureusement, la plupart des sites visités ne respectent pas ce souhait. Le CECIL propose donc de compléter ce *Do Not Track* par des outils plus protecteurs pour résister à ces pratiques.

Il faut déjà relever que, depuis novembre 2015, la navigation privée sur Firefox protège par défaut l'utilisateur contre un grand nombre d'opérations de traçage.

Pour compléter cette protection et la rendre opérationnelle hors navigation privée, il suffit d'installer des modules qui vont bloquer au maximum les tentatives des sites pour obtenir des données sur l'utilisateur et le suivre dans ses navigations sur le Web.

5.1 uBlock Origin un "Adblock", contre le traçage publicitaire

Le plus célèbre d'entre eux est "Adblock Plus" qui fait disparaître des navigations la majorité des encarts publicitaires. Toutefois en raison de ses nouvelles pratiques commerciales critiquables, le CECIL conseille plutôt d'installer un de ses clones : uBlock Origin. Celui-ci reprend des éléments du code source d'Adblock Plus, qui est sous licence libre, sans les fonctionnalités critiquées et est plus efficace que celui-ci. 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" anti-traçage. Ces listes sont tenues à jour automatiquement et peuvent aussi être complétées par l'utilisateur. 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").

Un troisième niveau consiste à se protéger des 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. Pour s'en protéger :

Dans les préférences du module, onglet "Mes filtres" et ajouter ce groupe de filtres : ||google-analytics.com/ga.js$third-party
||plus.google.com/u/0/_/streamwidgets/||*fbcdn.net/*$domain=~facebook.com ||facebook.com/*$third-party* ||*twitter.com/*$third-party

Pour les utilisateurs de Facebook, pour bloquer la fonctionnalité permettant aux participants à une discussion de voir si des messages ont été "vus", il faut aussi ajouter :

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

5.2 Disconnect.me, un complément nécessaire

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 protégeront contre un grand nombre de traqueurs.

5.3 Privacy Badger, le petit nouveau 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 utilisateurs. 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 constitue sans nul doute un module de choix pour se protéger toujours plus !

Ces trois 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.

5.4 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 l'expérience de la CNIL sur les traces (sur son site) 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.
- 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 utilisateurs plus avisés et prêts à réaliser les configurations nécessaires, il est enfin recommandé d'utiliser NoScript.

Pour aller plus loin :

- pour connaitre les traces basiques, mais nombreuses laissées lors des navigations et les limites de l'anonymat : anonymat.org,
- une autre présentation des modules permettant de contrôler ses informations sur Internet sur "contrôle tes données" géré par la Quadrature du Net,
- un article de bestvpn en anglais, *recommended firefox security extensions*, 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 noire" ou de "liste blanche". Ainsi, si on souhaite permettre à un site de nous tracer on peut choisir de désactiver le blocage sur ce site en particulier (liste blanche).

> 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 noire).

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

- Sur le blog Ohax! : *Oubliez le pachydermique Adblock Plus, uBlock Origin est arrivé !*, détaillant les avantages de uBlock Origin.

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".

6. 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").

Côté utilisateur, il faut toutefois prendre d'autres précautions.

La première précaution est d'utiliser un mot de passe qui ne soit pas facilement devinable par un attaquant (date de naissance, identique à l'identifiant…), mais il faut également se prémunir des techniques de "force brute" consistant à essayer systématiquement de très nombreux mots de passe. Pour réduire ce risque, il faut que le mot de passe soit suffisamment long (strict minimum 8 caractères) et comporte 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.

Pour l'utilisateur, 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 du seul utilisateur. Au lieu de la date et lieu de naissance on pourrait mettre "NéàdouzeH13unmardi". Cette phrase peut être liée ou non au service utilisé (de façon non évidente) pour que l'on s'en souvienne. Pour une boîte 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. Il s'agit là d'un compromis avec le risque que la découverte d'un mot de passe entraîne 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'utilisateur. 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 paradoxalement permettre d'accéder au compte encore 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'utilisateur, 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 maître" 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 possibilité est d'utiliser un gestionnaire extérieur. Ce logiciel, à installer sur son ordinateur, gérera 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 maître, le seul à devoir être mémorisé par l'utilisateur. 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 modifier après, par précaution.

De nombreux gestionnaires sont disponibles ; Lastpass, passreminder, Password Safe, onepassword… En raison de sa gratuité, de sa 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". C'est une référence en la matière.

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,
- 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, un gestionnaire de mots de passe certifié par l'ANSSI,
- 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*,
- 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.

7. Des outils alternatifs en ligne

Une nouvelle tendance se dessine. De plus en plus d'utilisateurs 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*"

7.1.1 Les avantages pour l'utilisateur :

- 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 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, c'est vous le produit !"*.

7.1.2 Les inconvénients pour l'utilisateur :

Ses données sont généralement exploitées à des fins de traçage publicitaire, d'établissement de profils de consommateurs et l'utilisateur 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 utilisateurs.

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

- de perte de contrôle sur ses outils, par exemple avec l'impossibilité de les adapter à ses besoins,
- de dépendance à un prestataire extérieur,
- de ne pas pouvoir récupérer ses données pour les réutiliser dans un service concurrent,
- de 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 utilisateurs 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 utilisateurs 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",
- 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 deux derniers services permettent aisément d'éviter d'utiliser le service Google Doc pour l'essentiel des usages.

En 2015, cette offre de services s'est étoffée avec des 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 différents utilisateurs autour du logiciel Owncloud. 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 utilisateurs et sans exploitation de leurs données.

7.2.2 D'autres services alternatifs

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

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 de ses utilisateurs,
- le logiciel libre Owncloud, 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 utilisateurs. 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 tous !

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*,
- DegooglisonsInternet.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 dispose aussi d'une interface dédiée plus complète : map.project-osrm.org,
- pour une autre alternative à Skype, on peut citer le récent projet Tox.im ou Mumble.

8. Des hébergeurs de messagerie alternatifs : se réapproprier ses courriels.

Avoir une messagerie électronique est devenu incontournable. Nos courriels sont le reflet de nos vies, le besoin de contrôle et de sécurité est donc total. 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 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 par les gouvernements.

Pour se protéger contre ces intrusions liberticides dans sa 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 qui garantirait réellement la vie privée et la sécurité de ses utilisateurs 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 :

- Mailoo.org, hébergement associatif français gratuit avec une incitation à soutenir *via* une donation,
- Tutanota.com, hébergement privé allemand gratuit,
- Autistici/Inventati, hébergement associatif italien militant (en anglais) gratuit avec une incitation à soutenir *via* une donation,
- ProtonMail.com, hébergement privé suisse gratuit.

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 coopérative d'Ouvaton,
- les offres commerciales d'OVH et de Gandi.

La plupart de ces solutions sont comparées sur des aspects de sécurité et de 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 réglementations liées notamment au Patriot Act, les hébergeurs français le seront à celles de la "loi renseignement".

Ces solutions reposent majoritairement sur le logiciel libre RoundCube pour la gestion à distance des courriels. Si on préfère gérer ses courriels sur son ordinateur, 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 utilisateurs 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 :

- Own-Mailbox un projet visant à installer simplement un serveur mail.

D'autres hébergeurs de messagerie intéressants à découvrir :

- Sud-Ouest.org (rien à voir avec le journal homonyme), hébergement associatif français à prix libre,
- Toile-Libre.org et le mail Singularity, hébergement associatif français à prix libre,
- le service No-log.org de GlobeNet, hébergement associatif français gratuit avec une incitation à participer *via* donation,
- 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,
- Openmailbox, hébergement associatif français gratuit avec une incitation à soutenir *via* donation.

9. Des réseaux sociaux alternatifs

9.1 Promouvoir et défendre des réseaux sociaux respectueux des utilisateurs

Il ne semble pas nécessaire de rappeler les dangers potentiels de Facebook pour la vie privée 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 ?*", ou encore Gizmodo.fr, "*pour 10 bonnes raisons de quitter Facebook*"... et ce même pour les utilisateurs non-inscrits 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'inscrits. 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 convaincus de l'intérêt des réseaux sociaux, mais qui souhaitent lutter contre cette hégémonie et utiliser des services plus respectueux des libertés des utilisateurs, le CECIL recommande les alternatives suivantes.

9.2 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'utilisateurs actifs. 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 !

9.3 SeenThis et Identi.ca, des alternatives à Twitter

Twitter est un bel outil, qui dispose d'une importante communauté facilitant la transmission d'informations ciblées, permettant de signaler facilement des articles pertinents et faire connaitre des événements. 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 utilisateurs et les exploite commercialement à des fins de traçage, de revente massive et d'établissement de profils commerciaux. Si l'entreprise semble un peu plus respectueuse que ses deux grandes soeurs, Facebook et Google, son usage conséquent lui confère malgré tout beaucoup de pouvoir.

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

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

Ces outils présentent des différences d'utilisation conséquentes et force est de reconnaitre qu'ils ne constituent pas encore une alternative complètement fonctionnelle, mais doivent être soutenus. Il est possible, dans une période transitoire, de les utiliser conjointement à Twitter *via* des "passerelles" permettant la publication simultanée sur les différentes plateformes.

Pour aller plus loin :

- à noter qu'il existe un autre logiciel décentralisé de réseau social similaire à Diaspora : Movim.eu,
- Zinc, le réseau social du Monde Diplo s'appuyant sur SeenThis.

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 de se cacher derrière un pseudo qui masque notre véritable identité pour discuter ou commenter, 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 du titulaire de la connexion, il peut donner à une autorité l'identité de celui qui se connecte à un site ou établit une communication. Tout ordinateur transmet aussi automatiquement à tous les services en ligne un certain nombre d'informations (dont le *user-agent* qui correspond 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 faciliter l'apparition de 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 : protection contre une surveillance abusive (qu'elle soit privée ou publique), échanges protégés dans le cadre de professions ou activités sensibles (avocat, journaliste, militant, lanceur d'alerte...), etc.

Des outils existent pour protéger sa confidentialité 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 accédera à notre place aux contenus désirés. On empêche ainsi le service final ou tout autre intermédiaire de connaitre sa véritable identité.

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 oignon") 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 ses 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 dont la tâche se trouve singulièrement complexifiée.

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).

Lancé en 2002, son objectif principal est donc d'anonymiser les communications sur Internet. Ainsi, une requête à un serveur va transiter par de nombreux ordinateurs ou serveurs répartis dans le monde rendant impossible à 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 noeud 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 :

- tout individu pour préserver sa vie privée,
- tout professionnel pour garantir la confidentialité du transfert de ses informations,
- des lanceurs d'alertes et des journalistes pour se protéger et informer depuis des zones dangereuses, sans risques de censure par certains pays ou opérateurs,
- des militaires pour garantir l'intégrité de l'information,
- etc.

Même si on se soucie peu de protéger sa vie privée, utiliser TOR sans réel besoin d'anonymat, protège indirectement 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*, disponible pour Windows ou pour un autre système 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 tous ! Une autre croyance courante est celle de la lenteur 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) aucune lenteur ne se fait plus particulièrement sentir pour un usage classique 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 sa confidentialité. Au-delà de failles pouvant être découvertes dans le futur, certaines mauvaises pratiques peuvent toutefois révéler l'identité par :

- la transmission d'informations, personnelles ou non lors des navigations (utilisation du même pseudo ou mot de passe, syntaxe similaire…),
- l'échange de contenus *via* l'usage du protocole *BitTorrent*) (*via* TOR) du fait de ses caractéristiques, qui en plus de risquer de saturer le réseau, identifie ses utilisateurs. Il est donc proscrit d'employer TOR dans ce cas,
- 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 (voir les prochaines fiches).

Utiliser TOR ne permet donc pas de tout faire si l'on souhaite protéger totalement 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 vidéo, une absence d'identification durable sur les sites consultés (mais c'est le but), une personnalisation des sites (langage, etc.) dépendante du dernier noeud réseau avant la requête, etc.

Il faut noter que si le dernier noeud 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 malveillantes.

De plus, si quelqu'un est ciblé directement par une surveillance de son réseau local ou de son ordinateur (infecté par un virus par exemple) le surveillant 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.

Des pages non respectueuses des lois françaises sont accessibles par de telles adresses (comme *"The Silk Road"*), en même temps cela permet également à des dissidents 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/ qui est une liste de liens ".onion" assez représentative de ce que l'on peut trouver dans ces services cachés.

10.1.5 Les autres réseaux anonymisants

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 recommande 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 petit 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 des communications. En souscrivant à leurs services, si la communication en direction du VPN est parfaitement sécurisée (chiffrement...), il sera impossible de déterminer qui a accédé à tel ou tel contenu sur Internet, les informations d'identification transmises étant celles du VPN de l'entreprise.

Cette sécurité 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 coût, 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 protégera 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),
- pour soutenir le développement de noeuds 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 en français.

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,
- Korben.info, *Quel VPN choisir*, qui relaie notamment un tableau d'analyse assez détaillé (malheureusement sur GoogleDoc et en anglais),
- Torrentfreak.com, *Which VPN services take your anonymity seriously? 2016 edition*,
- parmi les VPN payants les plus communément cités comme techniquement fiables (pas forcément juridiquement) on trouve notamment HideMyAss.com, localisé en Angleterre, qui conserve les *logs* quelque temps, 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),
- 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 :

- Anonymat.org, une page française sur l'anonymat sur Internet,
- Movilab.org, page Wiki Anonymisation navigation Internet résumant les enjeux de l'anonymat sur Internet et ses méthodes,
- 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.

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. 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 cryptologie : protéger ses données par le chiffrement

L'idée générale est de "brouiller" le contenu des données par des méthodes mathématiques. On parle alors de "cryptologie" ou science du secret, 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.

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

Gnu-Linux

Pour l'utilisateur 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). L'intérêt de chiffrer intégralement son disque dur pour un besoin minimal de sécurité n'est pas évident, notamment en raison de la quantité de calculs nécessaire susceptible de ralentir l'ordinateur. Pour un usage personnel classique, le CECIL conseille vivement de chiffrer au moins le dossier personnel avec un code fiable (telle une phrase de passe). Ce code protégera 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 des logiciels libres :

- Pour Windows, le logiciel diskcrypto :

  Une fois téléchargé, puis installé en suivant les instructions, il suffira de choisir la partition de disque dur à chiffrer, de cliquer sur "*Encrypt*", de choisir de préférence le "Chiffrement AES" (*Advanced Encryption Standard*) et de définir une phrase de passe sûre et mémorisable. Le logiciel chiffre alors la partition du disque, ce qui peut prendre du temps. La phrase de passe sera demandée à chaque démarrage et la partition sera devenue inaccessible sans elle.

- Pour Mac OS X, le logiciel AESCrypt.

Dans le cas où Filevault serait malgré tout utilisé, il faut faire attention à l'utiliser correctement.

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 des archives compressées et chiffrées de documents rapidement *via* la méthode AES256 considérée comme fiable.

- Pour 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 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".

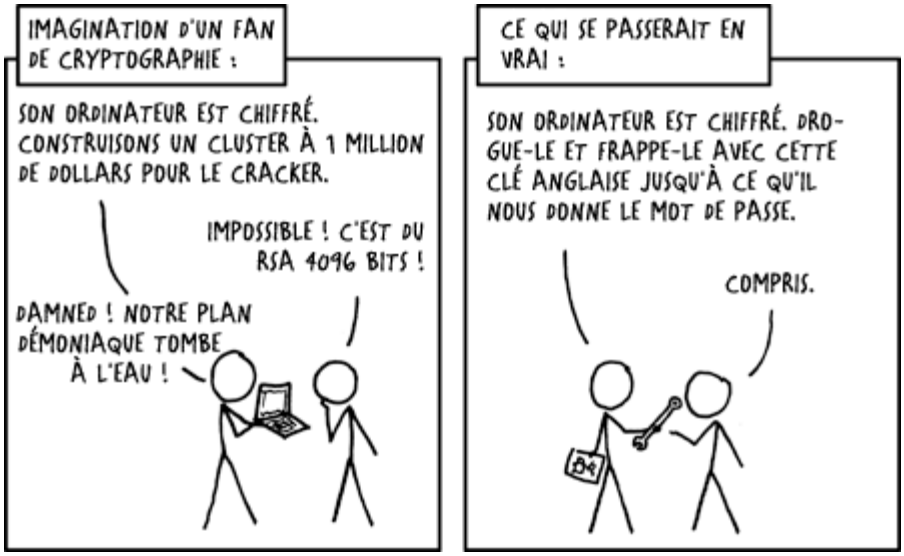
- Pour Mac OS X, il s'agit du logiciel 7zx.

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,
- 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

- 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,
- le CECIL signale aussi les logiciels CipherShed et Veracrypt pour chiffrer ses données, utilisable sous les trois systèmes d'exploitation. Il s'agit de *fork* du logiciel libre *TrueCrypt* qui autrefois faisait référence, mais a été victime d'un épisode étrange en 2014. Ces deux logiciels s'appuient 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. Il permet aussi de supprimer d'autres traces (fichiers temporaires, historiques de navigation, précédentes recherches...).

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. On parle ici de cryptographie.

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 correspondants (*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 correspondants, qui une fois refermés par eux ne peuvent être ouverts que par le détenteur de la clé privée (celui 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* qui découle du protocole *SSL* (*Secure Sockets Layer*), on parle souvent de "SSL/TLS") couramment utilisé sans en avoir toujours conscience en naviguant sur Internet. C'est le "s" du "HTTPs" ou le petit cadenas qui apparaît dans le 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 Wi-Fi 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 du message (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, un indice demeure : l'existence d'une communication entre A. et B. Pour dissimuler cette information 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 oeuvre 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 correspondants 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 clef" puis dans la nouvelle fenêtre ouvrir le menu "Générer" -> "Nouvelle paire de clefs".
>
> Choisir l'adresse concernée, indiquer une phrase de passe, qui protégera 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 clé et que l'on récupère leurs clés publiques.

Pour cela soit on reçoit la clé publique directement et il suffit d'ouvrir le fichier *via* Enigmail, soit il faut la chercher dans un annuaire.

L'accès à ces annuaires se fait dans la fenêtre "Gestion des clefs" d'Enigmail. Cliquer sur "Serveurs de clefs" 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 correspondant, 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 possibilité fonctionne quel que soit le Webmail, de préférence ceux conseillés par le CECIL sous RoundCube, SquirrelMail, et 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 clé 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 apparaît 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 !

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*.

Les solutions en la matière sont plus limitées. Il existe néanmoins 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, en cours de développement, évoqué fiche 7 offre un service de conversation audio totalement chiffré,
- 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 correspondants 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 l'EFF (en français) pour chiffrer ses courriels,
- un autre tutoriel très accessible sur le chiffrement des communications sur "Contrôle tes données", *GnuPG*,
- 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,
- l-homme-numerique.ze-forum.com, *HOWTO - Chiffrer/Déchiffrer des courriels avec un webmail - version avancée, un tutoriel d'utilisation de 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 d'Enigmail sont constamment en train d'être améliorés,
- en complément à la fiche 8 sur les hébergeurs de courriels alternatifs, le Webmail suisse ProtonMail.ch propose à la fois un chiffrement GPG par défaut entre titulaires de compte Proton Mail, une gestion de GPG 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 est toutefois encore largement en développement et les inscriptions sont contingentées. Le projet CaliOpen souhaite aussi mettre en oeuvre de tels mécanismes parmi d'autres méthodes de protection.