Les fiches pratiques du CECIL pour réduire les risques liés à la surveillance

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 vous 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. Deux outils fondamentaux : le système d'exploitation et le navigateur.

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 (sans l'avoir explicitement demandé), facturés insidieusement. 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. Aller sur la fiche.

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 limiter des possibilités malicieuses (portes dérobées, contrôle par un éditeur commercial…). En conséquence, la « communauté » exerce un fort contrôle sur ces logiciels. Dans une société où l'informatique est omniprésente, la maitrise de nos outils est un enjeu majeur. Ce combat est aussi mené par les défenseurs du logiciel libres. Aller sur la fiche.

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 clefs du Web et certains en profitent pour enregistrer beaucoup de données sur les recherches effectuées et tracer leurs utilisateurs. 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 DuckDuckGo ou d'IxQuick. Aller sur la fiche.

4. L'historique de navigation et les cookies.

Par défaut, lors d'une navigation sur Internet, des données sont enregistrées dans votre ordinateur en fonction de vos recherches et connexions à des pages. Il s'agit notamment de l'historique de vos visites et des cookies. Si ces données peuvent faciliter vos navigations futures, vous risquez aussi 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 vous suivre dans vos navigations. Heureusement, il est possible de limiter, contrôler ou supprimer ces enregistrements. Aller sur la fiche.

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'Adblock ou Disconnect, sont disponibles. Aller sur la fiche.

6. Les mots de passe.

Outil clef 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 complexifier leur mémorisation pour se prémunir d'intrusion ou d'usurpation d'identité non souhaitées. Aller sur la fiche.
.

7. Les outils en ligne, 8. hébergeurs de courriels et 9. 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'information... 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 vos données, le CECIL vous recommande différents outils, plus respectueux de la vie privée et des libertés, au travers de trois fiches.

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

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

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 commercial. 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 est important de savoir qu'il existe 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 vous permettent de :

- économiser le prix d'une licence Windows,
- vous protéger un peu plus des risques d'attaque (plus le système est utilisé plus il est visé -tel Windows-),
- donner un coup de jeune à un ordinateur un peu ancien… et cela sans perdre en fonctionnalité 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, pour Ubuntu, vous trouverez ici des informations et des tutoriels vidéos en français. Il en va de même pour Linux Mint. Si vous redoutez ces opérations qui, sans être trop complexes, demandent quand même quelques compétences, des bénévoles seront ravis de vous aider lors d'événements appelés « fêtes d'installation » (*install party*) ou, plus spécifiquement des « Ubuntu party ». La pluparts 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 clef 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 clefs : 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 Adblock Edge, 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 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 facilitant l'installation de mesures techniques de protection des contenus (*Encrypted Media Extensions*). Malgré ces concessions, ce navigateur reste un excellent choix pour protéger la liberté 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 (quoi que moins développés), mais sans compromission face aux mesures techniques de protection ni au financement par Google. IceCat intègre de surcroit 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, Linux Mint, Debian, Fedora. Les sites des principaux navigateurs cités : Firefox, Palemoon, Midori, IceCat. 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.

2. Les logiciels libres

Les systèmes d'exploitation Gnu-Linux comme les navigateurs Firefox ou IceCat présentés par ailleurs 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 propriété 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, 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 désigne 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 si vous n'avez pas l'intention de modifier ces logiciels libres, en les utilisant vous les soutenez et contribuez à leur diffusion et popularité en incitant d'autres à les améliorer. De plus, vous pouvez 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 de 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 précédant et de recréer un clone sans celles-ci (voir l'exemple d'Adblock Plus -> Adblock Edge). 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. N'hésitez pas à vous 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, nous vous invitons à 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 clefs 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 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 ; https://duckduckgo.com ; 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, cliquez sur l'icône en forme de loupe de la barre de recherche de Firefox et cliquez sur 'Ajouter « DuckDuckGo »'. Il vous faudra ensuite recliquez sur la loupe, cliquez sur « Modifier les paramètres de recherche ». Dans l'interface ouverte, vous pourrez choisir « DuckDuckGo » comme moteur par défaut.

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, vous évitez la personnalisation des contenus, qui introduit un biais de confirmation, et obtenez 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 vous 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 votre requête »*, vous serez automatiquement redirigé vers le thesaurus. Point notable, vous pouvez même accéder à Google sans être tracé (« !g votre 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.

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 ; https://ixquick.com ; 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 à votre navigateur, rien de plus simple, il suffit d'ouvrir ce lien et de cliquer sur « installer » (la version HTTPS de préférence). La procédure détaillée pour DuckDuckGo fonctionne également.

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 votre ordinateur.
- Il n'y a pas de récupération à votre insu d'informations personnelles, 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.

Vous bénéficiez ainsi des résultats des principaux moteurs de recherche sans pour autant leurs livrer vos données personnelles. En pratique, Ixquick réalise les requêtes à votre place. 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.

Les limites d'Ixquick

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 votre adresse IP à la recherche, Google aura quand même connaissance de caractéristiques techniques de la recherche (mots-clefs, heure, indication linguistique, affichage de la publicité, etc.) Sans être parfaits, 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, Searx, ou encore Yacy..

3.3 Yacy ; http://yacy.net/fr/ ; 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.

3.4 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 vous cherchez fréquemment un article de Wikipédia, une définition précise sur le Portail lexical du CNRS ou une aide à la traduction sur Linguee, nul est besoin de l'intermédiation d'un moteur généraliste, que ce soit Google ou DuckDuckGo. Vous pouvez ajouter ces moteurs à votre barre de recherche. Sur Firefox, il vous suffira dans la majorité des cas de :

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

Ensuite, vous pourrez cliquer sur la loupe quand vous vous apprêtez à faire une recherche puis cliquer sur l'icône du moteur voulu pour cette seule recherche. Vous pouvez aussi regarder si le moteur est référencé dans cette base 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. Si vous êtes simplement intéressés par la remise en cause du monopole de Google, vous pouvez aussi voir à Exalead, Qwant ou encore WolframAlpha, intéressants à d'autres égards, sans toutefois avoir un réel engagement éthique. La fiche Wikipédia française listant les moteurs de recherche protecteurs de la vie privée. Des articles et compléments sur DuckDuckGo : http://articles.softonic.fr/duckduckgo-moteur-de-recherche-anonyme-oubliez-google http://www.netpublic.fr/2014/04/apprendre-a-utiliser-duckduckgo-moteur-de-recherche-qui-respecte-la-vie-privee-6-tutoriels/ http://donttrack.us/ 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 :

> Inscrivez « about:config » dans la barre d'adresse puis validez. Validez que vous « ferez attention ». Ensuite vous réaliserez un clic droit (sur Ctrl + Clic sans souris) n'importe où, puis cliquez sur Nouvelle Valeur booléenne. Indiquez « browser.search.showOneOffButtons ». Par défaut la valeur devrait être en « false ». Validez et redémarrez Firefox.

4. L'historique de navigation et les cookies

4.1 Présentation

Internet Explorer, Google Chrome, Mozilla Firefox (évoqués ici) récupèrent un grand nombre d'informations stockées sur **votre** ordinateur durant votre navigation. Il s'agit de traces concernant vos recherches et les pages des sites visités. Ces traces comportent :

- un historique de navigation 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 Internets et mots de passe…),
- des données conservées visant à faciliter les navigations ultérieures (cache, préférences de sites, cookies).

L'ensemble de ces informations constitue « 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 nécessaire pour réaliser des achat 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 les boutons de partage des réseaux sociaux, présents sur de nombreuses pages, permettent à Facebook, Google et Twitter de tracer vos visites sans même les cliquer. Pour se préserver de cette intrusion, c'est par ici !

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 dans l'onglet « Fichier / Ouvrir une nouvelle fenêtre de navigation privée ».

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

> dans l'onglet « Vie privée » des options, choisissez le paramètre « ne jamais conserver l'historique ».

Sans utiliser la navigation privée, vous pouvez également supprimer vos traces locales régulièrement. Sur Firefox, il suffira de cliquer sur l'onglet « Historique », puis « supprimer l'historique récent ». Vous pourrez alors choisir les éléments que vous souhaitez supprimer ou conserver et définir la période de suppression. Vous pourrez ainsi supprimer toutes vos traces temporaires et ne conserver que vos favoris et autres mots de passe enregistrés sur votre machine. L'utilisation de la navigation privée ou la suppression manuelle de l'historique sont des fonctions importantes en particulier si vous partagez votre ordinateur avec d'autres. C'est par exemple le cas pour l'utilisation d'un ordinateur public. Il s'agit là de protéger votre vie privée face aux personnes ayant accès au même ordinateur qui peuvent être vos proches ou non.

4.3 Les limites de la gestion locale de ses traces.

L'utilisation de la navigation privée ne vous protégera toutefois pas de nombreuses possibilités de surveillance de vos communications ou de vos données de connexion par :

- des sites web que vous consultez ;
- des employeurs ou gestionnaires locaux de votre accès réseau selon le paramétrage choisi ;
- votre FAI (Fournisseur Accès Internet) ;
- des mouchards malveillants, virus ou intrusions sur votre machine ;
- d'une interception en direct de la communication.

Même s'il s'agit d'une protection limitée, il est important de connaître et maîtriser la gestion de ses propres traces. Cela vous permettra d'éviter que vos proches ou un tiers indésirable ne prennent connaissance d'informations que vous jugez personnelles. Cela ne vous empêchera toutefois pas d'être tracé et profilé par des 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 vers 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. 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 (présenté ici).

5. Les protections contre le tracage

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 votre « temps de cerveau disponible » 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 me tracez pas). Nous vous conseillons de l'utiliser, sur Firefox :

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

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

Le CECIL vous propose des solutions pour résister à ces pratiques. Il vous suffit d'installer des petits modules qui vont bloquer au maximum les tentatives des sites pour obtenir des données sur vous-même et vous suivre dans vos navigations sur le Web.

5.1 Adblock, contre le traçage publicitaire.

Le plus célèbre d'entre eux est « Adblock Plus » qui fait disparaître de vos navigations la majorité des encarts publicitaires. Toutefois en raison de ses nouvelles pratiques commerciales critiquables, le CECIL vous conseille plutôt d'installer un de ses clones : Adblock Edge. Celui-ci reprend le code source d'Adblock Plus, qui est sous licence libre, sans les fonctionnalités critiquées, ni réelle volonté commerciale. Pour l'installer facilement sur Firefox, il vous suffit de l'ajouter via ce lien.

Il s'installe avec, par défaut, une liste de base de publicités bloquées (*Liste-FR+EasyList*) qui va stopper la plupart des publicités sur Internet. Cette liste est tenue à jour automatiquement et peut aussi être complétée par l'utilisateur. Par ailleurs, il est possible d'ajouter des filtres anti-traçage. Pour cela, il vous faudra rajouter la liste « EasyPrivacy ».

> Celle-ci est disponible ici (puis cliquez sur « Ajouter EasyPrivacy à Adblock Plus »).

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 connaître les sites que vous avez visités. Pour s'en protéger :

> Cliquez sur le logo d'Adblock, choisissez préférences de filtre puis onglet « filtres personnalisés » et ajoutez 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

Si vous êtes utilisateur de Facebook, pour bloquer la fonctionnalité permettant aux participants à une discussion de voir si vous avez lu les messages, vous pouvez aussi ajouter :

> ||facebook.com/ajax/mercury/change*read*status.php$xmlhttprequest

5.2 Disconnect.me, un complément nécessaire.

Comme Adblock ne bloque pas tous les dispositifs de traçage, Disconnect.me est un bon complément. Même si Adblock 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, cliquez ici, puis « ajoutez Disconnect.me ».
>
> Pour compléter l'installation : Cliquez sur l'icône « D » de Disconnect.me et cliquez sur celle à côté de « Content » pour bloquer aussi les traqueurs contenus dans les articles.

Ces deux extensions vous protégeront contre un grand nombre de traqueurs.

Si toutefois vous craigniez de voir vos requêtes suivies à travers le Web, d'autres précautions sont nécessaires.

5.3 Quelques autres extensions intéressantes

- En naviguant sur Internet, vous transmettez par défaut des caractéristiques de votre navigateur et de votre système d'exploitation (vous pouvez le constater en réalisant l'expérience de la CNIL sur les traces), pour éviter d'être trop transparent et choisir les informations transmises, vous pouvez utiliser User Agent Switcher. Ce module vous permettra de faire croire que votre 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 vos communications de façon chiffrée dès que cette option est disponible et réduit ainsi les risques d'écoutes.
- Privacy Badger, de l'EFF, dont l'objectif est de combiner les avantages des différentes extensions protectrices de la vie privée (dont Adblock et Disconnect) au sein d'une seule

extension. Il s'agit toutefois d'un projet récent, pas totalement opérationnel, et qui n'a pas pour vocation de bloquer toutes les publicités.
- 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 prêts à réaliser les configurations nécessaires, il est recommandé d'utiliser NoScript.

Pour aller plus loin :

- Pour connaître les traces basiques, mais nombreuses laissées lors de votre navigation et les limites de l'anonymat visitez anonymat.org
- Une autre présentation des modules permettant de contrôler ses informations sur Internet sur contrôle tes données.
- Un article de bestvpn en anglais sur les extensions relatives spécifiquement à la sécurité.
- Sur la question du

La plupart des extensions précédemment mentionnées, et notamment Adblock permettent d'exclure ou d'inclure certains éléments du filtrage. On parle de « liste noire » ou de « liste blanche ». Ainsi, si vous souhaitez permettre à un site de vous tracer vous pouvez choisir de désactiver le blocage sur ce site en particulier (liste blanche).

> Pour cela cliquez sur le logo d'Adblock Edge et cliquer sur « Désactiver pour… » A l'inverse, si certains éléments ne sont pas automatiquement bloqués par les listes installées vous pouvez les bloquer spécifiquement (liste noire). Pour cela, réalisez un clic droit sur l'élément souhaité et cliquez sur « bloquer … avec Adblock ».

- Sur la question du « Do Not Track », nous vous invitons à consulter les liens suivant :
  - la page du projet (en anglais)
  - un explication de l'EFF (en anglais)
  - la page wikipedia française

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 individu mal intentionné obtient votre mot de passe, il pourra usurper votre identité avec des conséquences potentiellement très graves (récupération de vos 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 vous avez peu de prise (évitez au moins les opérateurs qui conservent et/ou transmettent votre mot de passe en « clair »).

De votre côté, vous devez également prendre des 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 votre mot de passe soit suffisamment long (minimum 8 caractères) et comporte des minuscules, des majuscules, mais aussi des chiffres et caractères spéciaux. Un opérateur sérieux mettra en place des mesures protectrices : nombre limité de tentatives, utilisation de « captcha »… Cela ne vous dispense pas pour autant de vous protéger de votre côté.

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 de vous seul. Au lieu de votre date et lieu de naissance vous pourriez mettre « NéàdouzeH13unmardi ». Cette phrase peut être liée ou non au service utilisé (de façon non évidente) pour que vous en rappeliez. Pour votre boîte courriel par exemple : « IciJereçois~10mails/jour ». La phrase de passe permet de concilier les avantages d'un mot de passe complexe tout en le mémorisant plus facilement.

Sur des services non critiques où une compromission de votre compte ne serait pas vraiment problématique (sans élément relatif à votre vie privée, données bancaires, base de contact, etc.), évitez malgré tout d'utiliser le même mot de passe. Au minimum, adoptez 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 en particulier si vous êtes personnellement visé.

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 qui vous sera transmis par SMS.

La contrepartie de cette amélioration de la protection de votre compte est la transmission de données supplémentaires (numéro de téléphone dans le cas précédant, 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 de votre téléphone peut paradoxalement permettre d'accéder à votre compte encore plus facilement.

Les méthodes mixtes sont très intéressantes en termes de sécurité pure. Il faudrait pouvoir s'assurer qu'elles sont bien mises en œuvre et que l'autre élément demandé ne soit pas problématique en soi. Si 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 vous fabriquez vos mots de passe, leur mémorisation est toujours un défi. Une solution est d'utiliser des gestionnaires de mots de passe qui offrent une forte protection sans effort de mémorisation.

Attention, toutes les solutions disponibles ne sont pas équivalentes. Ainsi, la quasi totalité des navigateurs offrent 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 à votre navigateur peut prendre connaissance de tous vos mots de passe enregistrés. Pour pallier ce risque, il est nécessaire de créer un « mot de passe maître » protégeant l'accès aux mots de passe. Il faudra l'indiquer à chaque session ou accès, mais c'est une protection indispensable. La procédure est détaillée ici.

> En bref, il s'agit d'aller dans « outils (ou édition sous Gnu-Linux), options, sécurité, utiliser un mot de passe maître », idéalement une phrase de passe.

Une autre possibilité est d'utiliser un gestionnaire extérieur. Ce logiciel, à installer sur votre ordinateur, gérera la mémorisation des mots de passe à votre place. Si les pratiques varient d'un logiciel à l'autre, les plus sérieux chiffrent vos mots de passe qui ne deviennent accessibles qu'en fournissant le mot de passe maître qui sera le seul à mémoriser. Il doit être complexe et respecter les règles précédemment évoquées. Vous pourrez ensuite stocker dans le gestionnaire tous vos mots de passe, même les plus complexes sans devoir les mémoriser. Le logiciel peut aussi proposer des mots de passe complexes que nous vous conseillons tout de même 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, nous vous recommandons le logiciel « Keepass ». C'est 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 sur les mots de passe.
- Un tutoriel de la CNIL pour installer et utiliser Keepass, un gestionnaire de mots de passe certifié par l'ANSSI.
- Une fiche de la CNIL s'agissant du piratage de ses comptes sociaux *via* mot de passe.
- Quelques règles de base sur la création de mots de passe.
- Une présentation de Zythom sur les méthodes « de base » permettant de casser des mots de passe pour comprendre ce dont il faut se prémunir.
- Un article sur les séquences de mots de passe à éviter (en anglais).
- Les limites des questions secrètes pour la récupération des mots de passe.
- Les velléités des constructeurs de remplacer les mots de passe par d'autres méthodes, notamment par des méthodes biométriques sont évoquées ici.
- Pour sortir des seules considérations de sécurité et de protection, nous vous invitons à consulter les deux articles suivants du New York Times (en anglais) et de Rue 89 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 ». Le service est alors fourni par un prestataire.

7.1 Le « *Cloud computing* »

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 sur 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 rappelez-vous : *« si c'est gratuit, c'est vous le produit ! »*.

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 même souvent à créer de la valeur pour l'entreprise sans pourtant être rémunéré pour cela ! Par exemple, Google Street utilise vos 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 vos données appartiennent peut être à des entreprises moins attachées au respect de votre vie privée que vous-même.

L'informatique en nuage comporte donc des risques sérieux 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 vous trouverez des alternatives à de nombreux outils utilisables sur Internet et vous trouverez par là une fiche dédiée à la gestion des courriels et par ici une 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 vidéo 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 vous recommande.

La dégooglisation d'Internet : les projets Framasoft.

L'association Framasoft, évoquée par ailleurs 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 Stud 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 parfaitement remplacement à « 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.

Il y en a d'autres que nous vous invitons à découvrir : Framindmap, Framanews...

Pour Framasoft, il s'agit vraiment d'offrir des services efficaces et viables garantissant les libertés des utilisateurs et sans exploitation de leurs données.

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,
- Hello, la récente messagerie vidéo intégrée à Firefox de la Fondation Mozilla. Si le partenariat avec la société Telefonica peut être critiqué, il s'agit néanmoins d'une alternative viable 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. Malheureusement, actuellement il n'existe pas encore d'offre d'hébergement gratuit pour les données que vous souhaiteriez héberger « dans le nuage ». Owncloud fonctionne toutefois parfaitement avec les hébergeurs évoqués également dans la fiche 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. Alors n'hésitez pas 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.
- Dégooglisons Internet, 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, vous pouvez par le site principal calculer normalement un itinéraire, si vous voulez une interface dédiée pour cela vous pouvez aussi utiliser OSRM.
- Pour une autre alternative à Skype, on peut citer le récent projet Tox.

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

Avoir une messagerie électronique est devenu incontournable. Nos courriels sont le reflet de notre vie, le besoin de contrôle et de sécurité est donc total. Pourtant, l'immense majorité des particuliers opte, par manque d'information, par praticité 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.

8.1 Des hébergeurs alternatifs

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, hébergement privé allemand gratuit,
- Autistici/Inventati, hébergement associatif italien militant (en anglais) gratuit avec une incitation à soutenir *via* une donation.

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 par ici : www.prxbx.com/email/.

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

À vous de 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".

8.2 Une réappropriation de ses courriels

Ces solutions reposent majoritairement sur le logiciel libre RoundCube pour la gestion à distance des courriels. Si vous préférez gérer vos courriels sur votre 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 nous recommandons.

Une autre solution est d'installer votre propre serveur local, sur un ordinateur dédié (permettant d'héberger votre 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 reconnaître 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 nous vous invitons à découvrir voire à soutenir.

Pour aller plus loin :

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

- Un article évolutif présentant les différents services existants
- Les raisons de l'abandon du projet, pourtant prometteur, Hemlis
- Own-Mailbox un projet visant à installer simplement un serveur mail chez vous

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/Mail Singularity, hébergement associatif français à prix libre
- Le service No-log de GlobeNet, hébergement associatif français gratuit avec une incitation à participer *via* donation
- Vmail, 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
- Kolab Now, 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 votre vie privée tant ceux-ci sont documentés, et ce même si vous configurez correctement votre compte. Un téléchargement de vos données devrait vous en convaincre, si nécessaire. Voir par exemple les explications du site sortir de Facebook, *"la vie privée un problème de vieux cons ?"*, ou encore "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 vous recommande ces alternatives :

9.2 Diaspora, une alternative à Facebook

Le logiciel Diaspora est une alternative viable 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 vos données vont être réparties de façon chiffrée. Vous pouvez participer à ce réseau sans connaissance particulière en utilisant n'importe lequel de ces points d'inscription (appelés Pod) disponibles ici.

Si vous souhaitez même éviter que vos 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 vos amis à en faire de même vous pouvez toutefois changer cet état de fait et continuer de bénéficier de cet outil sans voir vos données offertes en pâture aux publicitaires, aux *data brokers* et à la surveillance des États.

Le CECIL vous recommande d'utiliser et de soutenir le Pod de l'association Framasoft évoquée par ailleurs, qui s'appuie sur Diaspora : Framasphère. 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 connaître 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 de vos 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 important 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

Ces outils présentent des différences d'utilisation conséquentes et force est de reconnaître qu'ils ne constituent pas encore une alternative complètement fonctionnelle, mais doivent être soutenus. A noter que si vous souhaitiez, dans une période transitoire les utiliser conjointement à Twitter des "passerelles" existent pour publier vos contenus simultanément sur les différentes plateformes.

Pour aller plus loin :

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