GUIDE DE SURVIE
à destination
DES AVENTURIERS D'INTERNET

ou comment protéger ses libertés en milieu numérique "hostile"

Ligue des **droits de l'Homme**
FONDÉE EN 1898

Le CECIL
Centre d'études sur la citoyenneté l'informatisation et les libertés
www.lececil.org
contact@lececil.org

Juillet 2016

Avec le développement des réseaux sociaux, des achats en ligne, des courriers électroniques, des objets connectés, etc. les possibilités d'atteintes à notre vie privée et d'utilisation de nos données personnelles ont considérablement évolué. Mal informés, résignés, contraints ou consentants faute de mieux, dans un contexte général qui nous incite à les révéler, nous avons revu à la baisse la protection de nos données personnelles. Pourtant, les nombreux risques liés au traitement de nos données nous concernent directement ; nous sommes susceptibles de les subir quotidiennement. Voici juste quelques exemples :

- **un profilage complet de nos pratiques de consommation et de nos navigations, aussi bien en ligne que par l'accumulation de nos données bancaires, de cartes de fidélité, etc. permettant de nous influencer par des publicités ciblées, et donc en pratique de nous manipuler dans nos actes d'achats, dans le recours à un service ou par la création d'un besoin. L'objectif est de tenter de devancer nos désirs, de prédire nos actions et d'infléchir nos décisions, et donc notre libre arbitre ;**
- **ce harcèlement peut même se poursuivre « dans la rue » sur des panneaux publicitaires communicants équipés de capteurs (dits « beacons ») qui espionnent nos appareils portables géolocalisés ;**
- **discriminations tarifaires en fonction de notre adresse IP ou de nos précédentes données de connexions (IP – Tracking et Cookie Tracking) ;**
- **risques d'atteintes à notre droit à la tranquillité ;**
- **risques d'usurpation d'identité ou d'utilisations frauduleuses de nos données bancaires ou d'autres éléments relatifs à la vie privée ayant une valeur patrimoniale ou morale.**

Une surveillance abusive est à craindre, qu'elle soit ciblée ou massive, qu'elle soit réalisée par des États, des administrations ou des entités privées, de la grande entreprise à l'individu isolé, avec selon les cas des risques :

- **relatifs aux dérives vers un état totalitaire ;**
- **de sanctions préventives sans justification matérielle basées sur des données passées ;**
- **de pratiques discriminatoires par la rupture d'égalité de traitement en raison d'un profil atypique ou de données incomplètes ;**
- **de perte d'un bénéfice ou d'un avantage, en raison du dévoilement de données aussi bien au niveau administratif, commercial que salarial ;**
- **d'autocensure des opinions minoritaires, appelée « spirale du silence », aboutissant d'un point de vue sociétal à une remise en cause des libertés d'expression et d'opinion.**

« *Moi, je n'ai rien à cacher…* »

Peut-être, mais…

… ce n'est pas nous qui faisons les lois. Rien ne nous garantit que ce que nous faisons aujourd'hui et que nous considérons comme juste ne sera pas considéré illégal demain.

…Ce n'est pas nous qui surveillons non plus. Les pratiques des services de renseignements sont peu encadrées. Derrière des objectifs louables, tels que la lutte contre le terrorisme ou le crime organisé, peut se cacher une réalité différente, comme la surveillance à des fins politiques.

…Ce sont nos libertés qui sont réduites. Nous avons tendance à nous autocensurer lorsque nous nous savons soumis à une surveillance de masse, ce qui fait disparaître les idées minoritaires et entrave la démocratie.

…Et après tout, c'est notre vie privée. Même si toutes nos activités en ligne sont légales, nous sommes en droit de vouloir que ces activités ne soient ni accessibles, ni divulguées.

La protection des données personnelles relève, dans une large mesure, de réglementations nationale, européenne et mondiale, mais les États et les entreprises seront d'autant plus sensibilisés à la question que nous le serons !

Pour mieux maîtriser les informations exposées, protéger notre vie privée et nos libertés fondamentales cette brochure regroupe des fiches pratiques pour découvrir, pas à pas, des outils visant à assurer cette protection. Par exemple : en privilégiant des mots de passe complexes, en limitant les possibilités de traçage en ligne grâce à des outils appropriés, par le chiffrement ou encore en faisant le choix de logiciels libres et de services et sites Internet qui proposent un traitement respectueux de nos données personnelles.

Les fiches de cette brochure « **Défendre ses libertés en ligne face à la surveillance – Guide de l'aventurier en milieu numérique hostile** » ont été conçues par le Centre d'études sur la citoyenneté, l'informatisation et les libertés (CECIL). Leur mise en page est le fruit d'une collaboration avec la Ligue des droits de l'Homme (LDH).
L'illustration de couverture est l'œuvre de Péhä (lesptitsdessinsdepeha.wordpress.com), dessinateur libriste, et est aussi mise à disposition sous licence CC BY-SA v4.0. Les recherches et l'élaboration de ses fiches ont été principalement réalisées par Sylvain Steer, chargé de mission au CECIL.

Ces fiches sont consultables et seront tenues à jour sur www.lececil.org/fiches. Elles comportent des liens vers l'ensemble des articles et outils présentés.

FICHE 1

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

1.1
p. 14 Le système d'exploitation : l'alternative des distributions Gnu-Linux

1.2
p. 15 Le navigateur: un outil de base à choisir

FICHE 2

Les logiciels libres

2.1
p. 18 Présentation générale

2.2
p. 19 Les avantages des logiciels libres

2.3
p. 20 Les inconvénients des logiciels libres

2.4
p. 21 Une implication nécessaire de tous

FICHE 3

Les moteurs de recherche alternatifs

3.1
p. 23 DuckDuckGo : un moteur de recherche qui respecte la vie privée
p. 23 Les avantages d'utilisation de DuckDuckGo
p. 24 Quelques nuances

3.2
p. 24 Ixquick : un métamoteur protecteur européen
p. 24 Les avantages d'utilisation d'Ixquick
p. 25 Des limites

3.3
p. 25 Qwant : un projet français en développement

3.4
p. 26 Yacy : un projet à soutenir

3.5
p. 26 Les moteurs de recherche interne à des sites

FICHE 4

L'historique de navigation et les cookies

4.1
p. 28 Présentation

4.2
p. 29 Limiter les traces locales de ses communications sur Internet

4.3
p. 29 Les limites de la gestion locale de ses traces

FICHE 5

Les protections contre le traçage

5.1
p. 33 uBlock Origin, un « Adblock » contre le traçage publicitaire

5.2
p. 34 Disconnect.me, un complément nécessaire

5.3
p. 34 Privacy Badger, le petit nouveau de l'EFF

5.4
p. 34 Quelques autres extensions intéressantes

FICHE 6

Les mots de passe

6.1
p. 37 Les « phrases de passe »

6.2
p. 37 Les méthodes d'identification mixtes

6.3
p. 38 Les gestionnaires de mots de passe

FICHE 7

Des outils alternatifs en ligne

7.1
p. 40 Le « *Cloud computing* »
p. 40 Les avantages pour l'utilisateur
p. 40 Les inconvénients pour l'utilisateur

7.2
p. 41 Les outils alternatifs de travail collaboratif
p. 41 La dégooglisation d'Internet : les projets Framasoft
p. 42 D'autres services alternatifs

FICHE 8

Des hébergeurs de messagerie alternatifs : se réapproprier ses courriels

p. 45

FICHE 9

Des réseaux sociaux alternatifs

9.1
p. 48 Promouvoir et défendre des réseaux sociaux respectueux des utilisateurs

9.2
p. 48 SeenThis et Identi.ca, des alternatives à Twitter

9.3
p. 49 Diaspora, une alternative à Facebook

FICHE 10

L'anonymat sur Internet

10.1
p. 51 Usage du réseau TOR
p. 52 Pourquoi utiliser Tor ?
p. 52 Comment utiliser Tor ?
p. 53 Les limites
p. 53 Les services « cachés »
p. 54 Les autres réseaux anonymisants

10.2
p. 54 Usage d'un VPN

FICHE 11

Le chiffrement des données

11.1
p. 58 La cryptologie : protéger ses données par le chiffrement

11.2
p. 59 Chiffrer ses données stockées
p. 59 Chiffrer tout ou partie d'un disque dur ou d'un périphérique de stockage
p. 60 Chiffrer certains fichiers ou dossiers

11.3
p. 61 Limites au chiffrement des données

FICHE 12

Le chiffrement des communications

12.1
p. 64 Le chiffrement asymétrique

12.2
p. 65 Chiffrer ses navigations

12.3
p. 65 Chiffrer ses échanges personnels
p. 65 Chiffrer ses courriels
p. 67 Chiffrer ses autres échanges

PRÉSENTATION 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.

FICHE 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). 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 ».

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

FICHE 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 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.

DuckDuckGo

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 heures.
- 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-clefs, 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 viable pour protéger sa vie privée et ne semble pas cesser de s'améliorer.

Des mots de l'équipe : « *La philosophie de Qwant repose sur deux 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 DuckDuckGo ou 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 viable 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 webs 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 et fonctionnelle et facile à adopter.

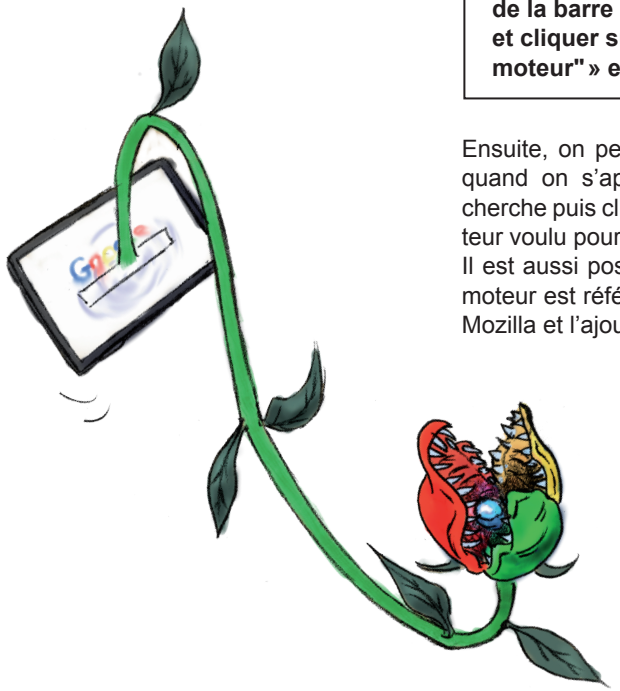
Son financement repose pour le moment sur les achats réalisés via son interface de « Shopping » sans causer donc de réels soucis relatifs à la vie privée.

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 est 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 :

- 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 un mois de test » ;
- D. Cuny, Rue89, « Qwant, le "Google français" ? On ne ricane pas, s'il vous plaît ».

FICHE 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 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 LeMonde.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.

FICHE 11

LE CHIFFREMENT DES DONNÉES

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

Ces techniques offrent d'énormes capacités de stockage et de communication, mais elles ont leur revers. Elles facilitent l'intrusion par quelqu'un de mal intentionné. 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 connaît pas le code. Évidemment, le « chiffre de César » est une technique très rudimentaire et facile à décrypter (à déchiffrer sans connaître 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.

Fiche 11
Le chiffrement des données

- 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 AES 256 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

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 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, *Libération*, 13 sept. 2015, « Cryptographie : la justice cherche la clé » ;
- S. Bortzmeyer, sur son blog, 1er 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, The Intercept (en anglais), nov. 2014, « 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 connaître 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...).

Fiche 11
Le chiffrement des données

12 FICHES POUR PROTÉGER SES LIBERTÉS EN MILIEU NUMÉRIQUE «HOSTILE»

1. Le système d'exploitation et le navigateur : deux outils fondamentaux
2. Les logiciels libres
3. Les moteurs de recherche alternatifs
4. L'historique de navigation et les cookies
5. Les protections contre le traçage
6. Les mots de passe
7. Des outils alternatifs en lignes
8. Des hébergeurs de messagerie alternatifs : se réapproprier ses courriels
9. Des réseaux sociaux alternatifs
10. L'anonymat sur Internet
11. Le chiffrement des données
12. Le chiffrement des communications

Ligue des droits de l'Homme

Ligue des droits de l'Homme
138 rue Marcadet – 75018 Paris
Tél. 01 56 55 51 00 – Fax 01 42 55 51 21
ldh@ldh-france.org – www.ldh-france.org

Le CECIL
Centre d'études sur la citoyenneté, l'informatisation et les libertés
www.lececil.org
contact@lececil.org

Le CECIL
Centre d'études sur la citoyenneté l'informatisation et les libertés
20 rue Saint Nicolas – 75012 Paris
contact@lececil.org – www.lececil.org