

Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications | Denis JACOPINI

Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications

Maintenant que la Loi Renseignement est votée, et en attendant la suite du processus législatif, apprenons à résister à la surveillance de masse avec quelques outils cryptographiques plus ou moins simples, mais efficaces et légaux.

Nous sommes le soir du mardi 5 mai, et c'est un jour funeste pour la démocratie. La France s'était autoproclamée « pays des Lumières » parce qu'il y a 250 ans notre pays éclairait l'Europe et le monde grâce aux travaux philosophiques et politiques de Montesquieu, qui prônait la séparation des pouvoirs, et de Voltaire et Rousseau.

À dater d'aujourd'hui, jour du vote en première lecture du projet de loi sur le renseignement, à cause d'une classe politique d'une grande médiocrité, s'enclenche un processus au terme duquel le peuple français va probablement devoir subir une loi dangereuse, qui pourrait s'avérer extrêmement liberticide si elle tombait entre de mauvaises mains, par exemple celles de l'extrême droite.

Même si la loi doit encore passer devant le Sénat puis peut-être revenir en seconde lecture à l'Assemblée Nationale, même si une saisine du Conseil Constitutionnel va être déposée par une soixantaine de courageux députés en complément de celle déjà annoncée par François Hollande, mieux vaut se préparer au pire, en imaginant que cette loi sera un jour promulguée. En faisant un peu de mauvais esprit, j'ai imaginé un nom pour le dispositif qui sera chargé de collecter nos données personnelles afin de détecter les comportements suspects : « Surveillance Totale Automatisée via des Systèmes Informatiques » et bizarrement l'acronyme est STASI !

Dès lors, à titre préventif et sans préjuger de l'avenir, il me semble important d'apprendre à protéger sa vie privée. Ceci passe par le chiffrement de ses communications, qu'il s'agisse d'échanges sur Internet ou via SMS, et cela peut se faire au moyen de différents outils à la fois efficaces et légaux.

Bien évidemment, les « vrais méchants » que sont les terroristes, djihadistes, gangsters et autres trafiquants connaissent et utilisent déjà ces outils : vous vous doutez bien qu'ils n'ont pas attendu ce billet de blog pour les découvrir...



Une boîte à outils pour protéger votre vie privée

Anonymat sur Internet

Pour protéger votre identité sur Internet et notamment sur le web, vous pouvez combiner l'utilisation d'un réseau privé virtuel, ou VPN, et de TOR, un système d'anonymisation qui nécessite l'installation d'un logiciel spécifique, TOR Browser. Je ne vous donne pas de référence particulière en matière de VPN, car l'offre est pléthorique.

MAJ : un lecteur m'a indiqué l'existence de La Brique Internet, un simple boîtier VPN couplé à un serveur. Pour que la Brique fonctionne, il faut lui configurer un accès VPN, qui lui permettra de créer un tunnel jusqu'à un autre ordinateur sur Internet. Une extension fournira bientôt aussi en plus un accès clé-en-main via TOR en utilisant la clé wifi du boîtier pour diffuser deux réseaux wifi : l'un pour un accès transparent via VPN et l'autre pour un accès transparent via Tor.

Chiffrement des données

Pour chiffrer le contenu de vos données, stockées sur les disques durs de vos ordinateurs ou dans les mémoires permanentes de vos smartphones, vous pouvez mettre en œuvre des outils tels que LUKS pour les systèmes Linux ou TrueCrypt pour les OS les plus répandus : même si TrueCrypt a connu une histoire compliquée, son efficacité ne semble pas remise en cause par le dernier audit de code effectué par des experts.

Je vous signale aussi que l'ANSSI – Agence nationale de la sécurité des systèmes d'information – signale d'autres outils alternatifs comme Cryhod, Zed !, ZoneCentral, Security Box et StormShield. Même si l'ANSSI est un service gouvernemental il n'y a pas de raison de ne pas leur faire confiance sur ce point ☐

Chiffrement des e-mails et authentification des correspondants

GPG, acronyme de GNU Privacy Guard, est l'implémentation GNU du standard OpenPGP. Cet outil permet de transmettre des messages signés et/ou chiffrés ce qui vous garantit à la fois l'authenticité et la confidentialité de vos échanges. Des modules complémentaires en facilitent l'utilisation sous Linux, Windows, MacOS X et Android.

MAJ : un lecteur m'a signalé PEPS, une solution de sécurisation française et Open Source, issue d'un projet mené par la DGA – Direction générale de l'armement – à partir duquel a été créée la société MLState.

Messagerie instantanée sécurisée

OTR, Off The Record, est un plugin à greffer à un client de messagerie instantanée. Le logiciel de messagerie instantanée Jitsi, qui repose sur le protocole SIP de la voix sur IP, intègre l'outil de chiffrement ZRTP.

Protection des communications mobiles

A défaut de protéger les métadonnées de vos communications mobiles, qu'il s'agisse de voix ou de SMS, vous pouvez au moins chiffrer les données en elles-mêmes, à savoir le contenu de vos échanges :

RedPhon est une application de chiffrement des communications vocales sous Android capable de communiquer avec Signal qui est une application du même fournisseur destinée aux iPhone sous iOS.

TextSecure est une application dédiée pour l'échange sécurisé de SMS, disponible pour Android et compatible avec la dernière version de l'application Signal. Plus d'information à ce sujet sur le blog de Stéphane Bortzmeyer.

MAJ : un lecteur m'a indiqué l'application APG pour Android qui permet d'utiliser ses clés GPG pour chiffrer ses SMS.

Allez vous former dans les « cafés Vie Privée »

Si vous n'êtes pas geek et ne vous sentez pas capable de maîtriser ces outils sans un minimum d'accompagnement, alors le concept des « cafés Vie Privée » est pour vous : il s'agit tout simplement de se réunir pour apprendre, de la bouche ceux qui savent le faire, comment mettre en œuvre les outils dont je vous ai parlé plus haut afin de protéger sa vie privée de toute intrusion, gouvernementale ou non.

Tout simplement, il s'agit de passer un après-midi à échanger et à pratiquer la cryptographie. Pour cela sont proposés des ateliers d'une durée minimum de 1 heure, axés autour de la sécurité informatique et de la protection de la vie privée.

Et comme le disent avec humour les organisateurs, « les ateliers sont accessibles à tout type de public, geek et non-geek, chatons, poneys, loutres ou licornes. ». Bref, le « café Vie Privée » est à la protection de la vie privée ce que la réunion Tupperware était à la cuisine ☐



Voilà, vous avez je l'espère suffisamment d'éléments pratiques pour commencer à protéger votre vie privée... en espérant vraiment que le Conseil Constitutionnel abrogera les points les plus contestables de cette loi et nous évitera d'avoir à déployer un tel arsenal sécuritaire.

PS : l'image « 1984 was not a manual » a été créée par Arnaud Velten aka @Bizcom.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : <http://www.zdnet.fr/actualites/loi-renseignement-la-bo-te-a-outils-pour-apprendre-a-protger-votre-vie-privee-en-chiffrant-vos-donnees-et-communications-39818894.htm>
Par Pierre Col