Quand on touche à la vie privée, c'est la démocratie qui est menacée (3/3)

Dans cette dernière partie, Eben Moglen nous donne quelques pistes pour protéger nos données personnelles.

Source : The Guardian, Privacy under attack: the NSA files revealed new threats to democracy

Traduction : Thérèse, fatalerrors (Geoffray Levasseur), goofy, audionuma, Diab, Paul, Omegax, lumi

> *L'incessante poursuite du profit qu'engendre l'extraction de données par tous les moyens légaux imaginables a causé une dévastation environnementale. Personne n'a jamais imposé les contraintes qui auraient dû exister dans l'intérêt de la protection contre la dégradation de l'environnement.*

On a tendance à condamner le partage à outrance. On entend souvent dire que le véritable problème de la vie privée est que les enfants vont bien trop loin dans le partage. Quand vous démocratisez un média, ce que nous sommes en train de faire avec le Net, les personnes ordinaires auront naturellement tendance à en dire plus qu'elles ne l'ont jamais fait. Ce n'est pas un problème. Dans une société libre, les gens devraient être protégés dans l'exercice de leurs droits à en dire autant ou aussi peu qu'ils le souhaitent.

Le véritable problème est que nous sommes en train de perdre l'anonymat de la lecture, ce pour quoi personne n'a signé.

Nous avons perdu la capacité de lire anonymement, mais cette perte nous est dissimulée à cause de la manière dont nous avons construit le web. Nous avons

donné au public des programmes appelés « navigateurs » que tout le monde peut utiliser, mais nous avons fait des « serveurs web » dont seuls les geeks peuvent faire usage — très peu de gens ont eu un jour l'occasion de consulter le journal d'un serveur web. C'est un immense échec de l'éducation à la technologie pour notre société, comme si l'on dissimulait aux enfants ce qui se passe quand des voitures entrent en collision et que les passagers ne portent pas de ceinture de sécurité.

Nous n'expliquons pas aux gens comment le journal d'un serveur web enregistre en détail l'activité des lecteurs, ni même combien on peut en apprendre sur eux simplement en sachant ce qu'ils *lisent*, et comment. À partir de ces journaux, vous pouvez savoir combien de temps chaque lecteur passe sur une page, comment il la lit, où il se rend ensuite, ce qu'il fait ou recherche à partir de ce qu'il vient de lire. Si vous pouvez rassembler toutes les informations qu'il y a dans ces journaux, alors vous commencez à posséder ce que vous ne devriez pas avoir.

Sans anonymat de la lecture il n'y a pas de liberté de l'esprit. C'est en effet littéralement l'esclavage. L'abolitionniste Frederick Douglass a écrit que la lecture était le chemin menant de l'esclavage à la liberté. Lorsqu'il décrit son propre cheminement dans ses mémoires, Douglass se souvient que lorsque l'un de ses propriétaires l'empêche de lire, « j'ai alors compris ce qui avait été pour moi une grande source de perplexité — à savoir, le pouvoir de l'homme blanc à asservir l'homme noir. » Et si chaque livre ou journal qu'il avait touché l'avait signalé ?

Si vous avez un compte Facebook, Facebook surveille chaque instant que vous y passez. Mais plus important encore, chaque page visitée contenant un bouton « J'aime » informera Facebook que vous avez lu cette page, que vous cliquiez sur ce bouton ou non. Si le journal que vous lisez chaque jour contient un bouton « J'aime » de Facebook ou les boutons de services similaires, alors Facebook ou les autres services vous regardent lire le journal : ils savent quels articles vous avez lus et combien de temps vous avez passé dessus.

Chaque fois que vous twittez une URL, Twitter la raccourcit pour vous. Mais il s'arrange aussi pour que toute personne cliquant dessus soit surveillée par Twitter pendant qu'elle lit. Vous n'aidez pas seulement des gens à savoir ce qu'on trouve sur le Web, vous aidez aussi Twitter à lire par-dessus l'épaule de toutes les personnes qui lisent tout ce que vous recommandez. Ce n'est pas transactionnel,

c’est écologique. C’est une destruction environnementale de la liberté de lire des autres personnes. *Votre* activité est conçue pour les aider à trouver les choses qu’elles veulent lire. L’activité de Twitter est de travestir aux yeux de tous la surveillance de la lecture qui en résulte.

Nous avons permis à ce système de grandir si rapidement autour de nous que nous n’avons pas eu le temps d’en comprendre les implications. Une fois que ces implications ont été bien pesées, les gens qui comprennent n’ont pas envie de parler, parce qu’ils ont un avantage et que cet avantage est dirigé contre vous. Puis la surveillance commerciale attire l’attention des gouvernements, avec deux résultats dont Snowden nous a apporté la preuve : la complicité et le vol qualifié.

Aussi pratiques, voire nécessaires, que leurs services puissent nous paraître, faute d’arriver à regagner la confiance de leurs clients, ils sont fichus.

Les entreprises spécialisées dans l’extraction de données croyaient, disaient-elles, qu’elles étaient simplement dans une situation de complicité avec le gouvernement. Après avoir créé des structures technologiques dangereuses qui fouillaient vos données personnelles, elles pensaient qu’elles étaient simplement engagées dans des négociations secrètes sur la quantité qu’elles devaient en livrer. C’était, bien sûr, un jeu où s’entremêlaient avidité et peur.

En gros, ce que les entreprises américaines d’extraction de données croyaient, ou voulaient nous faire croire qu’elles croyaient jusqu’à ce que Snowden les réveille, était qu’à travers leur complicité elles avaient obtenu l’immunité pour leurs vols qualifiés. Mais nous avons maintenant appris que leur complicité ne leur a rien rapporté. Elles nous ont vendu pour moitié, et le gouvernement a volé le reste. Elles ont découvert que ce qu’elles attendaient de l’honnêteté des grandes oreilles américaines, NSA et autres agences, elles étaient très loin de l’avoir obtenu. À l’évidence, l’attitude des grandes oreilles se résumait à : « Ce qui est à nous est à nous et ce qui est à vous est négociable… à moins que nous ne l’ayons d’abord volé. »

De même que l’industrie mondiale de la finance, les grandes entreprises d’extraction de données ont pris les promesses des grandes oreilles américaines trop au sérieux. C’est en tout cas l’interprétation charitable qu’on peut donner de leur conduite. Elles pensaient qu’il y avait des limites à ce que ferait le pouvoir.

Grâce à Snowden, que ce soit pour les extracteurs de données ou pour les grandes oreilles américaines, la situation n'est plus contrôlable politiquement. Ils ont perdu leur crédit, leur crédibilité, aux yeux du monde. Aussi pratiques, voire nécessaires, que leurs services puissent nous paraître, faute d'arriver à regagner la confiance de leurs clients, ils sont fichus.

Les problèmes environnementaux — tels le changement climatique, la pollution de l'eau, l'esclavage ou la destruction de la vie privée — ne se résolvent pas par des transactions entre individus. Il faut une union pour détruire l'esclavage. De même, l'essence de notre difficulté est l'union [1].

Cependant, une des caractéristiques des grands extracteurs de données est qu'il n'y a pas d'union des travailleurs, de syndicat, en leur sein ni autour d'eux. Ce sont maintenant des entreprises publiques, mais l'union des actionnaires ne contrôle pas efficacement les méfaits environnementaux qu'elles commettent. Ces entreprises sont d'une opacité remarquable en ce qui concerne leurs activités réelles et elles sont si profitables que les actionnaires ne tueront jamais la poule aux œufs d'or en remettant en cause l'éthique de leurs méthodes commerciales. Dans ces entreprises, un petit nombre d'individus puissants contrôle tous les votes ayant un effet concret ; la main d'œuvre n'a pas de voix collective.

Snowden a toujours été clair sur le fait que le remède à cette destruction environnementale est la démocratie. Mais il a aussi fait remarquer à plusieurs reprises que partout où les travailleurs ne peuvent pas s'exprimer et n'ont pas de voix collective, le droit du public à l'information n'est pas protégé. Quand il n'y a pas de voix collective pour ceux qui sont au sein de structures qui trompent et oppriment le public, alors quelqu'un doit agir courageusement de son propre chef.

Avant Auguste, les Romains de la république finissante savaient que le secret du scrutin était essentiel aux droits du peuple. Mais dans tous les pays du monde où se déroulent des élections dignes de ce nom, Google sait comment vous allez voter. Il est déjà en train de façonner votre paysage politique, dans vos fils d'actualité personnalisés, en fonction de ce que vous voulez lire, de qui vous êtes et de ce que vous aimez. Non seulement il sait comment vous allez voter, mais il vous aide en outre à vous conforter dans votre décision de voter ainsi — à moins qu'un autre message n'ait été acheté par un sponsor.

Sans anonymat de la lecture, il n'y a pas de démocratie. Je veux dire, bien sûr qu'il n'existe pas d'élection juste et libre, mais de manière plus fondamentale, je veux dire qu'il n'existe même plus d'autogouvernance libre.

Et nous sommes toujours très mal informés parce qu'il n'y a pas de syndicat cherchant à mettre en lumière les problèmes éthiques chez les extracteurs de données et que nous avons trop peu de Snowden.

L'avenir des extracteurs de données n'est pas le même pour tous. Google en tant qu'organisation s'est interrogé dès le début sur les implications éthiques de ses activités. Larry Page et Sergey Brin, les fondateurs de Google, ne sont pas tombés par hasard sur l'idée qu'ils avaient une obligation particulière à ne pas faire le mal. Ils comprenaient les dangers potentiels inhérents à la situation qu'ils créaient.

Il est techniquement possible pour Google de faire de Gmail un système véritablement sûr et respectueux du secret de la correspondance, quoique non anonyme. Les messages pourraient être chiffrés — en utilisant des clés publiques dans un réseau de confiance — au sein même des ordinateurs des utilisateurs, dans les navigateurs. Les messages stockés chez Google pourraient être chiffrés à l'aide d'algorithmes dont seul l'utilisateur et non Google posséderait les clés.

Google aurait à renoncer aux maigres profits de Gmail, mais ses actions seraient cohérentes avec l'idée qu'Internet appartient à ses utilisateurs à travers le monde. À long terme, il est bon pour Google de montrer, non seulement qu'il croit en cette idée, mais aussi qu'il agit en conséquence, car c'est la seule manière de

regagner la confiance des utilisateurs. Il y a beaucoup de personnes réfléchies et dévouées chez Google qui doivent choisir entre faire ce qui est bon et sonner l'alarme sur ce qui ne l'est pas.

La situation chez Facebook est différente. Facebook opère une mine à ciel ouvert de la société humaine. Scruter tout ce que chacun partage dans sa vie sociale en ligne et instrumentaliser le web pour surveiller tout ce que chacun lit en dehors du système est intrinsèquement immoral.

Mais de Facebook, nous n'avons besoin de rien d'autre que de vérité dans sa communication. Nul besoin de règles, de sanctions ni de lignes directrices. Nous avons seulement besoin de vérité. Facebook devrait s'incliner et dire à ses utilisateurs ce qu'il fait. Il devrait dire : « Nous vous observons à chaque instant que vous passez ici. Nous regardons chacun des détails de ce que vous faites. Nous avons mis le Web sur écoute avec des boutons "J'aime" qui nous informent automatiquement de ce que vous lisez. » À chaque parent, Facebook devrait dire : « Vos enfants passent des heures chaque jour avec nous. Nous les espionnons bien plus efficacement que vous ne serez jamais capables de faire. Et nous ne vous dirons jamais ce que nous savons d'eux. »

Rien que cela, juste la vérité. Ce serait suffisant. Mais la bande qui fait tourner Facebook, cette petite poignée de personnes riches et puissantes ne s'abaissera jamais au point de vous dire la vérité.

Mark Zuckerberg a récemment dépensé 30 millions de dollars pour acheter toutes les maisons autour de la sienne à Palo Alto en Californie — parce qu'il a besoin de davantage de vie privée. Cela vaut pour nous aussi. Nous devons manifester des exigences semblables en faveur de notre vie privée, aussi bien auprès des gouvernements que des entreprises.

Les gouvernements, comme je l'ai dit, doivent nous protéger de l'espionnage des gouvernements étrangers et doivent assujettir leurs propres écoutes domestiques aux règles établies par la loi. Les entreprises, pour regagner notre confiance, doivent être honnêtes sur leurs pratiques et leurs relations avec le pouvoir. Nous devons savoir ce qu'elle font réellement afin de décider si nous acceptons ou non de leur confier nos données.

Une grande confusion a été créée par la distinction entre données et métadonnées, comme s'il y avait une différence et que l'espionnage des métadonnées était moins grave. L'interception illégale du contenu d'un message viole le secret de son contenu. L'interception illégale des métadonnées du message viole votre anonymat. Ce n'est pas moins grave, c'est différent et la plupart du temps, c'est plus grave. En particulier, la collecte des métadonnées viole l'anonymat de la lecture. Ce n'est pas le contenu du journal que Douglass

lisait qui posait problème ; c'était que lui, un esclave, ait eu l'audace de le lire.

Le président peut s'excuser auprès des citoyens pour l'annulation de leur police d'assurance maladie, mais il ne peut se contenter d'excuses au peuple pour l'annulation de la Constitution. Quand vous êtes président des États-Unis, vous ne pouvez pas vous excuser de ne pas être du côté de Frederick Douglass.

Neuf votes à la Cour suprême des États-Unis peuvent remettre nos lois d'aplomb, mais le président des États-Unis possède l'unique vote qui importe en ce qui concerne la fin de la guerre. Car toute cette destruction de la vie privée par le gouvernement, organisée par-dessus un désastre écologique encore plus étendu causé par l'industrie, tout cet *espionnage*, c'est un truc de temps de guerre. Le président doit arrêter la guerre qui fait rage au sein du Net et nous dépossède de nos libertés civiles sous prétexte de vouloir priver d'asile les étrangers mal intentionnés.

Un homme qui apporte à la démocratie les preuves de crimes contre la liberté est un héros. Un homme qui vole la vie privée des sociétés humaines à son profit est un malfaiteur. Nous avons suffisamment d'infamie et pas assez d'héroïsme. Nous devons dénoncer cette différence de manière assez vigoureuse pour encourager d'autres personnes à faire ce qui est juste.

Nous avons vu qu'avec un acharnement digne des opérations militaires les grandes oreilles américaines sont engagées dans une campagne contre la vie privée du genre humain. Elles compromettent le secret, détruisent l'anonymat et nuisent à l'autonomie de milliards de personnes.

Elles font tout ceci parce qu'une administration américaine extraordinairement imprudente leur a attribué une mission – après avoir échoué à prévenir une attaque très grave de civils sur le territoire national, en grande partie à cause de sa négligence des mises en garde – en décrétant qu'elle ne serait plus jamais placée dans une situation où « elle aurait dû savoir ».

Le problème fondamental était le manque de discernement des politiques, pas celui des militaires. Quand des chefs militaires se voient assigner des objectifs, ils les atteignent au prix de tout dommage collatéral qu'on ne leur a pas explicitement demandé de ne pas dépasser. C'est pourquoi nous considérons le contrôle civil sur les forces armées comme une condition *sine qua non* de la démocratie. La démocratie exige également que les citoyens soient informés.

Le peuple des États-Unis ne veut pas devenir la police secrète du monde

Sur ce sujet, Snowden est d'accord avec Thomas Jefferson [auteur principal de la Déclaration d'indépendance américaine], ainsi qu'avec presque toutes les autres personnes qui ont un jour sérieusement réfléchi au problème. Snowden nous a montré l'extraordinaire complicité entre tous les gouvernements. Ils nous a montré, en d'autres termes, que les politiques souhaitées par les peuples sont partout délibérément contrariées par leurs gouvernements. Ce que veulent les peuples, c'est être protégés contre l'espionnage d'origine étrangère ; ils veulent aussi que les activités de surveillance menées par leur propre gouvernement pour assurer la sécurité nationale soient conduites sous l'examen minutieux et indépendant qui caractérise l'État de droit.

Par ailleurs, le peuple des États-Unis n'est pas prêt à abandonner son rôle de porte-drapeau de la liberté dans le monde. Il n'est pas prêt à se lancer à la place dans la dissémination des procédures du totalitarisme. Nous n'avons jamais voté pour cela. Le peuple des États-Unis ne veut pas devenir la police secrète du monde. Si nous avons dérivé dans cette direction parce qu'une administration imprudente a donné le pouvoir aux militaires, il est temps pour le peuple américain d'exprimer son opinion démocratique et sans appel [2].

Nous ne sommes pas les seuls au monde à avoir des responsabilités politiques exigeantes. Le gouvernement britannique doit cesser d'affaiblir les libertés civiles de son peuple et doit cesser d'utiliser son territoire et ses infrastructures de transport comme auxiliaires du mauvais comportement des forces armées américaines. Et il doit cesser de priver la presse de sa liberté. Il doit cesser de mettre sous pression les rédactions qui cherchent à informer le monde des menaces sur la démocratie, alors qu'il se montre assez compréhensif pour les éditeurs qui espionnent les familles de petites filles assassinées.

La chancelière allemande doit arrêter de parler de *son* téléphone mobile et commencer à s'exprimer sur la question de savoir s'il est bon de livrer tous les appels téléphoniques et tous les SMS d'Allemagne aux États-Unis. Les gouvernements qui sont régis par des constitutions protégeant la liberté d'expression doivent se demander, de toute urgence, si cette liberté continue à exister quand tout est espionné, surveillé, écouté.

Outre faire de la politique, nous devons absolument légiférer. Défendre l'État de droit est toujours un travail de juriste. En certains lieux, ces juristes auront besoin d'être extrêmement courageux ; partout ils devront être bien entraînés ; partout ils auront besoin de notre soutien et de notre implication. Mais il est également clair que soumettre les écoutes gouvernementales à l'autorité de la loi n'est pas le seul travail qui attend les juristes.

Comme nous l'avons vu, les relations entre les grandes oreilles militaires aux États-Unis, les grandes oreilles ailleurs dans le monde et les grandes entreprises d'extraction de données sont trop complexes pour être sans danger pour nous. Les révélations de Snowden ont montré que les géants américains de l'extraction de données ont été intimidés, séduits mais aussi trahis par les oreilles. Cela n'aurait pas dû les surprendre, mais ils l'ont apparemment été. Beaucoup d'entreprises gèrent nos données ; la plupart n'ont pas de responsabilité juridique envers nous qu'on puisse faire respecter. Il y a du travail pour les avocats là aussi.

Aux États-Unis, par exemple, nous devrions en finir avec l'immunité accordée aux opérateurs de télécommunication pour leur assistance dans les écoutes illégales. Cette immunité a été prorogée par la loi en 2008. Pendant la course à la présidence, Barack Obama avait dit qu'il ferait obstruction à cette législation. Or, en août 2008, quand il est apparu clairement qu'il serait le prochain président, il a changé d'avis. Non seulement il a jeté aux orties sa menace d'obstruction, mais en outre il a interrompu sa campagne pour voter en faveur de l'immunité.

Il n'est pas utile de polémiquer sur le bien-fondé de l'extension d'immunité. Nous devons fixer une date – éventuellement le 21 janvier 2017 [3] – après laquelle tout opérateur de télécommunications faisant affaire aux États-Unis et facilitant les écoutes illégales devrait être soumis aux règles du régime ordinaire de la responsabilité civile. Une coalition intéressante entre les juristes spécialisés dans les droits de l'homme et les avocats spécialisés en recours collectifs d'ordre commercial émergerait immédiatement, avec des conséquences très positives.

Si cette non-immunité était étendue aux opérateurs de réseau non américains qui font affaire aux États-Unis, par exemple Deutsche Telekom, cela aurait également d'immenses conséquences positives pour les citoyens des autres pays. Dans tout pays ou l'immunité existe aujourd'hui *de facto* et peut être levée, elle doit l'être.

Tous les systèmes juridiques connaissent bien les problèmes posés par l'énorme tas de données nous concernant qui sont entre les mains d'autres personnes. Les principes nécessaires sont invoqués chaque fois que vous portez vos vêtements chez le teinturier. Les juristes anglo-saxons appellent ces principes « droit du dépôt » *(law of bailment)*. Ce qu'ils entendent par là, c'est que si vous confiez vos affaires à d'autres, ces derniers doivent en prendre soin au moins autant qu'ils le feraient avec les leurs. À défaut, ils sont responsables de leur négligence.

Nous devons appliquer ce principe de la mise en dépôt, qu'il soit désigné sous ce nom ou un autre dans les vocabulaires juridiques locaux, à toutes les données que nous avons confiées à d'autres personnes. Cela rend ces dernières juridiquement responsables envers nous de la manière dont elles s'en occupent. Il y aurait un énorme avantage à appliquer aux données personnelles le droit du dépôt ou un droit équivalent.

Ces règles sont soumises au droit du lieu où le dépôt est effectué. Si le teinturier choisit de déplacer vos vêtements dans un autre lieu et qu'un incendie y survient, le lieu où le feu s'est déclaré est sans importance : la loi en vigueur est celle du lieu où il a pris en charge vos vêtements. Au contraire, les grandes entreprises d'extraction de données exploitent en permanence la ficelle de la règle du lieu *(lex loci)* pour leurs serveurs : « Oh, nous ne sommes pas vraiment dans le pays X, nous sommes en Californie, c'est là que nos ordinateurs se trouvent. » C'est une mauvaise habitude juridique. Cela ne les desservirait pas trop si on les aidait à en sortir.

Ensuite, il y a du travail à faire au niveau du droit public international. Nous devons tenir les gouvernements responsables les uns envers les autres afin de remédier à la dévastation environnementale actuelle. Le deux gouvernements les plus puissants du monde, les États-Unis et la Chine, sont maintenant fondamentalement d'accord sur leurs politiques vis-à-vis des menaces sur Internet. Le principe de base est le suivant : « Quel que soit l'endroit du net où existe une menace pour notre sécurité nationale, nous allons l'attaquer. »

Dans les années 50, les États-Unis et l'Union soviétique ont mis le monde en péril d'empoisonnement pour cause d'essais atmosphériques d'armes nucléaires. À leur crédit, ils furent capables de conclure des accords bilatéraux pour les interdire. Les États-Unis et le gouvernement chinois pourraient se mettre d'accord pour ne pas transformer l'humanité en zone de tir à volonté pour l'espionnage. Mais ils ne

le feront pas.

Nous devons chercher à obtenir réparation, par les voies politique et judiciaire, pour ce qui nous a été fait. Mais la politique et le droit sont trop lents et trop incertains. Sans solution technique, nous n'y arriverons pas, de même qu'on ne peut décontaminer l'air et l'eau ni agir positivement sur le climat à l'échelle mondiale sans changement technologique.

Partout, les entreprises utilisent des logiciels qui sécurisent leurs communications et une bonne part de ces logiciels sont écrits par nous. Par « nous », j'entends ici les communautés qui partagent du logiciel libre ou *open source*, communautés avec lesquelles je travaille depuis des décennies.

Les protocoles qui implémentent des communications sécurisées et que les entreprises utilisent entre elles et avec leurs clients (HTTPS, SSL, SSH, TLS, OpenVPN, etc.) ont tous été la cible de l'interférence des grandes oreilles. Snowden a apporté la preuve des efforts qu'ont fait ces dernières pour casser nos chiffrements.

Les oreilles américaines jouent avec le feu d'un désastre financier mondial. Si elles devaient réussir à compromettre les procédés techniques fondamentaux grâce auxquelles les entreprises communiquent de manière sécurisée, il suffirait d'une panne catastrophique pour qu'on bascule dans le chaos financier mondial. Leur conduite apparaîtra rétrospectivement comme aussi irresponsable du point de vue économique que la dévaluation de la monnaie romaine. Ce n'est ni plus ni moins qu'une menace pour la sécurité économique du monde.

La mauvaise nouvelle est qu'elles ont fait quelques pas en direction de la catastrophe irrémédiable. D'abord, elles ont corrompu la science. Elles ont secrètement influencé l'élaboration des standards techniques, affaiblissant ainsi la sécurité de tous, partout, afin de faciliter le vol de données à leur profit.

Ensuite, elles ont volé des clés, comme seuls les voleurs les mieux financés du monde peuvent le faire. Elles ont investi tous les endroits où est fabriqué du matériel intégrant des clés de chiffrement.

Début septembre [4], quand les documents de Snowden sur ce sujet ont été rendus publics, les ondes de choc se sont propagées dans toute l'industrie. Mais les documents divulgués ont également montré que les grandes oreilles sont encore

obligées de voler les clés plutôt que de casser nos verrous. Elles ne disposent pas encore de l'expertise technique suffisante pour casser les bases du chiffrement qui forme le socle de l'économie mondiale.

La publication des types de chiffrement que la NSA ne peut casser est la plus incendiaire des révélations de Snowden du point de vue des grandes oreilles. Aussi longtemps que personne ne sait ce qu'elles ne sont pas en capacité de lire, elles jouissent d'une aura d'omniscience. Lorsqu'on saura ce qu'elles ne peuvent pas lire, tout le monde va utiliser ce type de chiffrement et elles seront alors rapidement dans l'incapacité de lire quoi que ce soit.

Nous devons banaliser l'usage par les particuliers de technologies déjà adoptées par les entreprises, visant à sécuriser les communications et protéger la vie privée. Utiliser ces technologies doit être aussi simple qu'installer un détecteur de fumée

Snowden a dévoilé que leurs avancées sur les bases de notre cryptographie étaient bonnes mais pas excellentes. Il nous a aussi montré que nous avons très peu de temps pour l'améliorer. Nous devons nous dépêcher de remédier au tort qui nous a été fait par la corruption des standards techniques. À partir de maintenant, les communautés qui font les logiciels libres de chiffrement pour les autres doivent partir du principe qu'elles se heurtent aux « services nationaux du renseignement ». Dans ce domaine, c'est une mauvaise nouvelle pour les développeurs car il s'agit de jouer dans la cour des grands. Quand vous jouez contre eux, la plus minuscule des erreurs est fatale.

De plus, nous devons modifier l'environnement technique afin qu'il soit plus sûr pour les personnes ordinaires et les petites entreprises. Ceci consiste pour une grande part dans la diffusion de technologies que les grandes entreprises utilisent depuis une décennie et demie. Beaucoup trop peu a été accompli dans ce domaine jusqu'à présent. C'est comme si chaque usine de nos sociétés était équipée d'un système de protection perfectionné contre l'incendie – détecteurs de fumée, détecteurs de monoxyde de carbone, arroseurs, lances à haute pression, extincteurs de haute qualité – alors que les maisons du commun des mortels n'avaient rien de tout ça.

Nous devons banaliser l'usage par les particuliers de technologies déjà adoptées

par les entreprises, visant à sécuriser les communications et protéger la vie privée. Utiliser ces technologies doit être aussi simple qu'installer un détecteur de fumée, fixer un extincteur au mur, dire à vos enfants quelle porte prendre si l'escalier brûle ou même attacher une échelle de corde à la fenêtre du premier étage. Rien de tout cela ne règle le problème de l'incendie, mais s'il éclate, ces mesures simples sauveront la vie de vos enfants.

Il existe beaucoup de projets logiciels et de jeunes pousses qui travaillent sur des mesures de ce type. Ma FreedomBox, par exemple, est un de ces projets logiciels bénévoles. Et je suis enchanté de voir s'installer le début d'une concurrence commerciale. Les entreprises sont maintenant averties : les peuples du monde n'ont pas consenti à ce que les technologies du totalitarisme soient ancrées dans chaque foyer. Si le marché leur propose de bons produits, qui rendent l'espionnage plus difficile, ils les achèteront et les utiliseront.

Le courage de Snowden est exemplaire. Mais il a mis fin à ses efforts parce que c'est *maintenant* qu'il nous faut savoir. Nous devons accepter en héritage sa compréhension de cette situation d'urgence extrême. Nos hommes politiques ne peuvent pas se permettre d'attendre. Ni aux États-Unis, où la guerre doit s'arrêter. Ni dans le monde, où chaque peuple doit exiger de son gouvernement qu'il remplisse son obligation minimale de protection de sa sécurité.

C'est à nous de terminer le travail qu'ils ont commencé.

Nous avons besoin de décentraliser les données. Si nous conservons tout dans un seul grand tas – s'il y a un type qui conserve tous les messages électroniques et un autre qui gère tous les partages sociaux, alors il n'y a aucun moyen véritable d'être plus en sécurité que le maillon le plus faible de la clôture qui entoure ce tas.

En revanche, si chacun de nous conserve ce qui lui est propre, les maillons faibles de la clôture ne livreront à l'attaquant que les affaires d'une et une seule personne. Ce qui, dans un monde gouverné par le principe de l'État de droit, serait optimal : cette seule personne est la personne qu'on *peut* espionner car on a pour cela des éléments tangibles [5].

La messagerie électronique s'adapte admirablement bien à un système où personne n'est au centre et ne conserve tout. Nous devons créer un serveur de

messagerie pour monsieur tout-le-monde, qui coûte moins de cinq euros et puisse être posé à l'endroit où l'on plaçait ordinairement le répondeur téléphonique. Et quand il casse, on le jette.

La décentralisation des partages sociaux est plus difficile, mais reste à notre portée. Pour les personnes engagées et douées pour la technologie partout dans le monde, c'est le moment crucial, car si nous faisons notre travail correctement, la liberté survivra ; et quand nos petits-enfants diront « Alors, qu'avez-vous fait à cette époque ? », la réponse pourrait être « J'ai amélioré SSL. »

Snowden a fait avancer avec noblesse nos efforts pour sauver la démocratie. Ce faisant, il s'est hissé sur les épaules d'autres personnes. L'honneur lui en revient et à eux aussi, mais la responsabilité est nôtre. C'est à nous de terminer le travail qu'ils ont commencé. Nous devons veiller à ce que leur sacrifice ait un sens, veiller à ce que cette nation, toutes les nations, connaissent une renaissance de la liberté, et à ce que le gouvernement du peuple, par le peuple et pour le peuple, ne disparaisse pas de la surface de la Terre.

Cet article est dérivé de la série de conférences « Snowden and the Future », donnée à la Columbia Law School fin 2013 et disponible à l'adresse snowdenandthefuture.info. Une première traduction en français de ces conférences a été effectuée par Geoffray Levasseur et publiée à l'adresse www.geoffray-levasseur.org.

Notes

[1] En anglais, *union* signifie à la fois « union » et « syndicat ». Dans la suite du texte, ce mot est employé dans l'un ou l'autre sens.

[2] *Register their conclusive democratic opinion* : cela fait probablement allusion aux sites web où les habitants d'un État américain peuvent donner leur avis sur les politiques publiques de cet État. Par exemple : http://www.governor.iowa.gov/constituent-services/register-opinion/

[3] Date probable d'investiture du prochain Président des États-Unis.

[4] Septembre 2013.

[5] *Probable cause* : concept de droit aux États-Unis qui désigne l'existence d'éléments tangibles justifiant des poursuites pénales.

Crédits images

- *Privacy erased* par opensource.com (CC-BY-SA)
- *Faceboogator* par Dimitris Kalogeropoylos ((CC BY-SA 2.0)