« La nouvelle loi européenne sur le numérique est un jeu de dupes irréalisable »

[Source : limpertinentmedia.com]

Par **Amèle Debey**

Éric Filiol est un scientifique de formation. Après 22 ans dans l'armée de terre française, où il a toujours fait de la recherche et de l'opérationnel, il a travaillé dans le domaine des technologies de l'information et dans le monde du renseignement. Ses connaissances en cryptanalyse expliquent son expertise sur certaines histoires suisses liées au canton de Zoug et de Crypto AG. Cet ancien lieutenant-colonel est spécialisé en cryptologie et en virologie informatique, dans le domaine de la défense et de l'attaque. Titulaire d'un diplôme d'ingénieur en cryptologie (BESSSI), d'un doctorat en mathématiques appliquées et informatique de l'Ecole Polytechnique et d'une habilitation à diriger des recherches (HDR) en informatique, de l'Université de Rennes. Il possède également des qualifications OTAN dans le domaine du renseignement et de l'Info Ops. Et il est inquiet. Interview.

IMPORTANT : Cet article a été publié en libre accès en raison de l'importance de son contenu. Mais pour que [redacted] puisse continuer à fonctionner, n'oubliez pas de vous abonner ou de faire un don via le bouton prévu à cet effet sur la page d'accueil.
Seule votre aide nous permettra de continuer. Merci d'avance.

Amèle Debey, pour L'Impertinent : Selon vous, nos décideurs ne sont plus formés à la technique, qu'entendez-vous par là ?

Éric Filiol : Ils ne l'ont jamais été. Si je prends le cas spécifique de la France, les politiques font des études littéraires, juridiques ou en sciences humaines – ce qu'on appelle un peu ironiquement les sciences molles en France. Dans le monde francophone, la connaissance est classée en sciences dures et sciences humaines. Les premières (les mathématiques, la physique, la chimie, etc.) ont pour objet tout ce qui concerne la nature et l'univers. Les connaissances et les certitudes que l'on peut démontrer, que ce soit par le raisonnement (les mathématiques) ou l'expérimentation reproductible. Les

sciences humaines (droit, histoire, littérature…) sont tournées vers l'homme. Ce ne sont que des certitudes relatives et limitées dans le temps. Il n'y a aucun absolu possible : tout est à la fois vérité et mensonge. Les êtres humains ont toujours besoin de s'opposer les uns aux autres.

Pour revenir aux hommes politiques, il est rare de trouver des formations scientifiques. Je crois que la dernière en date était Madame Merkel, qui était chimiste. Peut-être que cela expliquait qu'elle soit un peu plus raisonnable que les autres. À la base, la formation des hommes politiques n'est absolument pas tournée vers la science. À dire vrai, cela tient peut-être au fait qu'en science, il est difficile de mentir. Quand les hommes politiques commencent à comprendre quelque chose, comme Thierry Breton par exemple, on le case à la Commission européenne pour être sûr qu'il ne gênera pas. On a un véritable problème de formation de nos élites. Et le problème n'est pas spécifique à la France. Autrefois, les hommes politiques savaient s'entourer de vrais spécialistes venant d'horizons différents, avec le service du bien commun et de l'État chevillé au corps. De nos jours, nous sommes dans l'information permanente, le buzz, la polémique, la recherche du lucre et autres. On n'interroge plus la légitimité des conseillers, leur expérience sur le terrain, mais d'autres considérations prennent le pas : la docilité, le copinage, l'effet de cour…

En science, une mauvaise décision peut être grave, mais elle l'est beaucoup plus dans les sciences humaines, en particulier dans le domaine des relations internationales et de la diplomatie. C'est une véritable catastrophe qui vaut de très nombreux déboires à la France actuellement. Dans le champ des relations internationales et du renseignement, les hommes politiques sont de plus en plus entourés de gens incompétents, beaucoup trop jeunes qui ne connaissent finalement rien alors qu'il existe des experts reconnus, sur le terrain depuis plus de vingt ans, qui parlent la langue et qui ne sont jamais consultés. Les jeunes conseillers se multiplient dans les ministères, qui donnent des avis absolument pas autorisés sur des affaires internationales ou sur des problématiques de zones – comment notamment en Afrique en ce moment – avec des impacts sur notre diplomatie et sur notre capacité à entretenir de bons rapports. Je suis convaincu que les hommes politiques sont désormais coupés de la réalité de manière préoccupante et qu'ils sont intoxiqués par des opinions et non plus des faits.

N'est-ce pas parce que la science implique le doute constant, quand la gouvernance demande des certitudes ?

Oui et non. La seule science pour laquelle on n'a pas de doute est les mathématiques. Et encore, tout dépend de l'ensemble des postulats de départ. C'est le mécanisme de la preuve. C'est la seule science exacte.

En sécurité informatique, beaucoup de choses reposent sur des suppositions qui n'ont jamais été démontrées (en sécurité par exemple, le célèbre problème P est différent de NP ?), mais on peut appliquer le principe de précaution. On peut quand même avoir des certitudes si ce principe de précaution est bien géré. En physique et en chimie ou autres sciences expérimentales,

l’expérience est ce qui nous confronte au réel. En informatique, c’est la capacité de l’homme à résoudre un problème ou pas. Là où ça coince, c’est que dans les sciences expérimentales, on est toujours à la merci du mécanisme de validation scientifique qui veut qu’autrui rejoue l’expérience. Or, on assiste à un accroissement du nombre de fraudes scientifiques dues aux enjeux (humains, financiers, pouvoir) impliqués, au manque de temps et/ou d’experts consciencieux pour analyser, vérifier, retester.

En sécurité de l’information, le problème est qu’on ne publie pas tout ce qu’on sait faire. Si quelqu’un sait attaquer un système de chiffrement ou un système d’information, les gens qui ont les meilleurs moyens – je pense aux agences gouvernementales – ne vont pas publier une telle connaissance pour conserver un avantage sur l’adversaire. Le gros problème de la sécurité vient finalement du fait que c’est un jeu à variables cachées permanent. C’est toute la différence entre le monde de l’attaque et celui de la défense. Je connais quelques techniques de cryptanalyse – ce qu’on appelle l’attaque des systèmes de chiffrement – qui ne sont toujours pas publiques, mais qui représentent un avantage non négligeable pour celui qui les connaît et j’imagine sans peine qu’il y en a beaucoup d’autres. Cela, bien sûr, représente un inconvénient pour celui qui est chargé de développer un système de chiffrement ou plus généralement de sécurité puisqu’il ne peut travailler qu’avec les connaissances ouvertes. La sécurité n’est prouvable que par rapport à ce que l’attaquant a bien voulu rendre public.

(Re)lire notre enquête : *Pass sanitaire mondial de l’OMS : l’inquiétude des spécialistes*

Dans le monde de l’informatique et de la sécurité, les dés sont pipés dès le début. Comme la cybersécurité est un enjeu mondial, les États et les industriels qui travaillent pour eux ont toujours intérêt à ce qu’il y ait un delta de connaissances entre celui qui peut attaquer et celui qui peut défendre. De nos jours, le marché des zero-day est le plus bel exemple (ce n’est pas le seul, il faut aussi considérer le cas des portes dérobées ou *backdoors*). Les zero-day sont des failles connues d’un petit nombre de gens, qui se négocient très chères pour les plus critiques (quelques millions de dollars l’unité) qui ne sont volontairement pas corrigées pour permettre des attaques. L’affaire Pegasus l’a démontré, entre autres nombreux exemples plus ou moins publics. Il y a donc des gens qui savent qu’il y a des failles, qui n’avertissent pas la communauté pour qu’elles soient corrigées, mais qui les vendent sous le manteau. Et on connaît les sociétés (environ une bonne dizaine) dont c’est le principal business, dont les premiers clients sont les États.

Donc s’il n’y a pas de gens formés à cela dans l’entourage des politiques, si eux-mêmes n’ont pas le choix, ni la prudence de s’entourer des bons experts ou d’une variété d’experts suffisante, ils prennent des décisions avec une vision biaisée.

Vous parliez de Thierry Breton tout à l’heure. Il est au cœur de l’actualité en ce moment avec l’instauration de la nouvelle loi européenne sur le

numérique qui se targue de « signer la fin d'une ère de non-droit ». Qu'en pensez-vous ? Est-ce réalisable sur le plan technique de surveiller tous ces géants du web et est-ce qu'on ne risque pas la censure sous couvert de lutte contre la désinformation ?

Ce n'est non seulement pas réalisable, mais c'est un jeu de dupes. Les lois européennes peuvent exister, à la fin si on veut les appliquer, on entre inévitablement dans un rapport de force avec les USA et de plus en plus avec la Chine. Les cas récents sont nombreux. L'Europe n'a pas de fondements politiques suffisant pour n'être rien de plus qu'une colonie numérique et économique de ces deux super puissances. Les GAFAM (les BATX, leurs équivalents chinois) sont trop puissants et surtout ils constituent une partie formidable de l'appareil de renseignement de ces États. La décision du 10 juillet 2023 montre toute la faiblesse de l'Europe et que, dans les faits, elle reste inféodée aux USA en se mentant à elle-même. La nomination par l'UE de Fiona Scott Morton (USA) pour surveiller les GAFAM est un autre bom exemple.

Les meilleurs hackers travaillent-ils pour des agences gouvernementales, selon vous ?

Il y en a. Cela dépend. Il y a un effet culturel. Les super puissances prennent les meilleurs là où ils sont. Elles regardent leur potentiel. La motivation peut être une véritable conscience nationale. Aux États-Unis, on va leur donner de gros salaires avec de fortes contraintes. S'ils sont un peu rétifs et anti-État, on passera à une méthode peut-être un peu plus musclée. En Chine et en Russie, par exemple, c'est plutôt le pistolet dans le dos. Encore qu'il y ait beaucoup de hackers patriotes. Il y a de nombreuses motivations différentes, l'argent étant la première et la plus forte.

> *« Le piratage est un carnage mondial dont nous ne pouvons pas encore mesurer les conséquences »*

Le problème c'est qu'en Europe, où on s'autoflagelle à l'envi, on veut être plus vertueux que la vertu elle-même. Dans le cas de la France, si on n'a pas fait une grande école d'ingénieur, on n'a pas voix au chapitre. C'est dramatique, car nous avons toute une communauté de hackers assez reconnue dans le monde. On a un système éducatif particulier et encore plus un esprit unique (un mélange d'esprit gaulois et de Descartes qui nous fait exceller dans le domaine de la sécurité) et on se coupe d'un certain nombre de visions.

Souvent, ces hackers sont dans des sociétés privées, qui cherchent à faire leur business, mais qui ne sont pas valorisés comme ils le devraient humainement et techniquement, parce qu'on a encore une sorte d'élitisme de mauvais aloi qui fait que l'on regarde plutôt la naissance que le potentiel. Ce n'est pas un hasard si certaines communautés étrangères sont plus fortes

que nous. Ce n'est pas forcément dû à la qualité, c'est simplement qu'ils sont beaucoup plus pragmatiques. En France, le pedigree de départ confronte très vite à l'effet « plafond de verre ».

C'est le cas dans le monde du travail en général, me semble-t-il…

Oui, c'est pour cela que je parlais de l'aspect culturel. Pourquoi la Suisse – qu'on identifie comme un monde de banquiers alors que la grande force de la Suisse c'est avant tout l'industrie. La Suisse c'est l'horlogerie, c'est la haute ingénierie. Nous Français sommes tellement ignares que l'on ne voit en la Suisse que les banques. Or, pourquoi la Suisse a réussi, comme l'Autriche et en partie l'Allemagne, c'est parce qu'elle sait encore fabriquer des ingénieurs maison. À travers l'alternance, mais pas celle à la française. Ils prennent les gens et en font de vrais ingénieurs tout au long de leur vie. C'est une approche culturelle différente. Ce n'est pas étonnant que ces pays-là soient en avance dans bien des domaines.

Il semblerait cependant que la Suisse soit un peu à la traîne sur le plan de la cybersécurité. Les sites de la Confédération ont récemment été victimes de sévères attaques par des hackers russes…

Que ceux qui n'ont pas été attaqués par les hackers russes lèvent la main ! Il n'y en a aucun. Les États-Unis et la France en sont victimes en permanence. Les autres n'en parlent pas. Il y a des attaques dont je ne peux pas parler parce qu'elles ne sont pas publiques, mais qui ont fait extrêmement de mal à des fleurons mondiaux de la sécurité, qu'ils soient européens ou américains. Les cas sont de plus en plus nombreux de vols de données très sensibles (données industrielles, mots de passe en clair de clients…). C'est un carnage mondial dont nous ne pouvons pas encore mesurer les conséquences totalement.

La Suisse n'est donc pas forcément en retard sur le plan de la cybersécurité ?

Non. Quand on regarde son système éducatif, entre l'ETH de Zurich, l'EPFL de Lausanne, la HEIG-VD d'Yverdon pour ne citer que ceux-là… il y a quand même de très beaux fleurons. Elle n'est pas en retard, elle fait moins parler d'elle. C'est différent. Mais, en termes d'attaque, elle n'est ni plus ni moins ciblée. J'aurais plutôt tendance à dire que son système fédéral fait qu'elle est un peu moins mal protégée.

> *« Le problème est la trop forte hégémonie d'un faible nombre d'acteurs technologiques »*

Le vrai problème – et il s'agit d'une hypocrisie mondiale – est que tous les systèmes sont attaqués parce qu'ils utilisent les mêmes technologies. On

utilise tous des technologies que plus personne ne maîtrise. Quand la Suisse se fait attaquer, c'est au niveau de systèmes dans lesquels il y a des failles. Ces failles ne sont pas suisses, mais américaines parce que la technologie est américaine. Il faut arrêter de voir la nationalité des victimes, mais plutôt celle de ceux qui fournissent les produits et les technologies. Les entreprises concernées, qui ne font rien de vraiment significatif sinon que de fournir des rustines sur les passoires qu'elles vendent, devraient être lourdement condamnées.

À tout concentrer dans les mains de quelques acteurs, le problème est que lorsque l'on trouve une faille dans un système que tout le monde utilise et qu'en plus on ne la documente pas trop, tous les clients en sont victimes. Le problème est la trop forte hégémonie d'un faible nombre d'acteurs technologiques, tellement puissants qu'ils ne veulent rien faire.

Pourquoi les Russes, les Ukrainiens, les Chinois, les Indiens ont ou sont en train de développer des technologies un peu plus souveraines et d'avoir leurs propres standards (en particulier en cryptologie) ? Parce qu'ils savent que d'une part ils ne peuvent pas faire confiance aux pays producteurs, mais surtout parce que dans l'informatique, la sécurité a été vers une uniformisation alors que l'on sait que, dans bien des domaines, la variété est un facteur de richesse et de sécurité. Le seul cas de la *backdoor* mise à la demande de la NSA dans un standard cryptologique (DUAL_ECC_RBG) résume à lui seul le propos.

Le simple concept de cybersécurité n'est-il pas une illusion ? Au bout du compte, doit-on accepter le fait que nous n'arriverons jamais à nous prémunir de ces attaques ?

C'est effectivement une illusion : on nous vend de la sécurité alors qu'elle n'est pas possible pour des tas de raisons : la concentration que je viens d'évoquer, le fait que les États n'ont pas intérêt à ce qu'il y ait une sécurité absolue.

Pourquoi la Commission européenne est en train de dire qu'il faut mettre des *backdoors* dans le chiffrement[1] ? Pourquoi le marché très juteux des zero-day est toléré ? La plus grosse société, autrefois française, est maintenant aux USA et travaille activement avec la NSA. Imaginons que demain nous ayons un système réellement inexpugnable. Les premiers à l'interdire seront les États. Les pays veulent amoindrir leur sécurité, mais être les seuls à en profiter. Douce illusion puisque les hackers sont là aussi.

La Suisse vient d'achever la révision de sa loi sur la protection des données. Elle se veut plus efficace que le Règlement général sur la protection des données européen (RGPD). Qu'en pensez-vous ?

Le RGPD est une vaste plaisanterie depuis le 10 juillet dernier. Jusque-là, on avait ce qu'on appelle la directive Schrems II. Avant, les États-Unis « garantissaient » la protection des données transférées par l'Europe grâce au *Privacy shield*[2], une garantie totalement illusoire pour ne pas dire un

mensonge éhonté. Max Schrems (*un activiste autrichien militant pour la protection des données, NDLR*) a démontré que ce n'était pas vrai. Que les services de renseignement américains puisaient dans les données européennes. Ce qu'avait également démontré Snowden : les données européennes font l'objet d'un pillage systématique. Depuis l'arrêt Schrems II, il est interdit de faire ce que l'on appelle un transfert hors Union européenne. Que ce soit aux États-Unis ou en Chine, puisque maintenant on a des plateformes de cloud chinoises (qu'une partie de l'industrie automobile française utilise, pour info).

En mars 2022, quand le président Macron et le reste de l'UE ont toqué à la porte du président américain pour dire « on veut bien se couper du pétrole et du gaz russe, mais il faut nous aider en nous en vendant », Joe Biden a accepté à la condition de rétablir l'accès aux données. Ce qu'on appelle un chantage.

> *« La Suisse va suivre la même voie que l'UE et se faire berner de la même manière »*

Le 10 juillet de cette année, Madame Von der Leyen, sans consulter le Parlement européen, a autorisé le transfert des données hors Union européenne. Et le plus beau, c'est qu'en cas de contestation, c'est une entité contentieuse américaine qui tranchera les cas litigieux !

Les données des Européens sont de bien meilleure qualité, car elles sont mieux collectées et traitées. Les données américaines sont des paillettes d'or dans beaucoup de boue, tandis que nous ce sont de grosses pépites. Elles représentent 5000 milliards de dollars par an. Les Américains ont donc gagné le 10 juillet 2023.

Mais le même problème va se poser aussi avec la Chine, car la deuxième plateforme mondiale de cloud est Ali Baba.

Malheureusement, il semble que si sur certaines choses la loi suisse va plus loin que le RGPD, elle comporte en revanche des points préoccupants (l'article 6 en est un). Concernant l'envoi des données vers les USA, le constat est que la Suisse va suivre la même voie que l'UE et se faire berner de la même manière. La notion de « sociétés américaines certifiées (dans le cas du DPF) » est une escroquerie intellectuelle destinée à masquer la faiblesse politique et économique des pays de l'espace européen. J'espère que Max Schrems repartira en guerre et que très vitre nous aurons un arrêt Schrems III pour y mettre fin.

En tant que citoyen, on a un peu le sentiment d'être démuni face à tout cela, que les révélations d'Edward Snowden n'ont rien changé…

Est-ce que le mot « citoyen » a encore un sens ? J'ai déjà reproché à des parlementaires d'avoir détruit le système éducatif, qui autrefois formait des citoyens critiques, pour en faire des consommateurs. Réponse d'un parlementaire dont je ne citerai pas le nom : oui, mais c'est quand même plus facile de gérer des consommateurs.

A-t-on vraiment un esprit citoyen ? Je ne dis pas qu'il a totalement disparu, mais on est noyé dans la masse. Quand on voit comment les gens s'abrutissent sur Tik Tok ou Instagram peut-on espérer vraiment les voir se poser les bonnes questions et s'interroger…

Cela ne va pas aller en s'arrangeant avec l'avènement de l'intelligence artificielle ?

On peut espérer que la bêtise naturelle soit plus forte que l'intelligence artificielle. Il n'est pas dit qu'Open AI fasse long feu : ils perdent 700 000 dollars par jour. Ils ont des serveurs monstrueux et ce n'est pas rentable. C'est une catastrophe écologique. Des data centers [Centres de données] monstrueux.

L'intelligence artificielle a prouvé son efficacité pour trouver des modèles quand il y en a beaucoup, mais lorsque ces modèles sont stables dans le temps : les lois de la nature. Dès lors que l'on applique l'intelligence artificielle à une activité humaine, cela ne fonctionne plus. Ce n'est pas modélisable, car les modèles sous-jacents ne sont plus stables.

C'est d'ailleurs toute la différence entre la sécurité et la sûreté. La seconde, c'est le code correcteur d'erreurs : je lutte contre une menace, mais qui n'est pas malveillante, c'est une loi statistique stable, donc on peut faire quelque chose (les codes correcteurs d'erreurs). L'attaquant, lui, il s'adapte. C'est le duel lance-cuirasse.

Nous, pays occidentaux, par fainéantise, sommes dans un confort coupable, la recherche du profit et du plaisir sans conscience aucune

> *« Nous, pays occidentaux, sommes dans un confort coupable, sans conscience aucune »*

Ce qui coûte très cher, c'est de requalifier en permanence les jeux de données. De comprendre comment évolue le cerveau humain. Les algorithmes sont connus depuis longtemps. Donc l'intelligence artificielle est un perroquet qui lit beaucoup et qui répète. Et le plus grave, c'est qu'il invente des faits.

Aux États-Unis, trois avocats ont été condamnés pour avoir demandé à ChatGPT d'écrire leur réquisitoire. Celui-ci a inventé des jurisprudences qui

n’existaient pas.

Ce que l’on ne sait pas, c’est que pour corriger les résultats, on a des armées de Kenyans et d’Ougandais qui souffrent et qui sont payés au lance-pierre afin de faire des corrections. L’intelligence artificielle est très efficace dans certains domaines, mais dans d’autres cas, on est en train de faire n’importe quoi et de perdre des savoir-faire.

Pas dans tous les pays : certains îlots ont le souci de maintenir la vraie connaissance. L’Afrique ne pourra pas se payer ChatGPT. Nous, pays occidentaux, par fainéantise, sommes dans un confort coupable, la recherche du profit et du plaisir sans conscience aucune. Tout cela n’est que la chronique d’une mort annoncée. Je vois notre niveau baisser globalement et on ferait mieux de s’intéresser à ce qui se passe ailleurs. La Chine a passé des lois pour préserver les enfants et les jeunes étudiants. D’autres pays maintiennent un système éducatif de qualité où les sciences ont une part encore importante.

La situation a-t-elle empiré depuis l’affaire Snowden ?

Considérablement. Il faudrait que je retrouve la phrase d’Obama, mais grosso modo, après cette affaire, il a dit maintenant que tout le monde le sait, on peut y aller.

Pour moi Obama a été le pire président pour les Européens. À chaque fois qu’il y a un président démocrate aux États-Unis, c’est une catastrophe pour l’Europe. Il a accru la surveillance globale comme aucun autre avant lui. C’était vraiment un vautour déguisé en agneau.

Pour info et dans l’indifférence générale, les archives Snowden ont été fermées (voir https://www.mintpressnews.com/intercept-snowden-archive/256772/) et leur exploitation arrêtée. Laure Poitras et Glenn Greenwald ont été marginalisés et écartés. Quel journaliste – après en avoir bien profité – a écrit un seul mot sur le sujet et s’en est ému ?

Vous m’avez l’air assez indulgent envers la Suisse, mais elle est en train de mettre en place le dossier médical électronique du patient que tous les professionnels de la santé seront tenus d’utiliser. Est-ce que ça ne pose pas un petit problème cette histoire ?

Si je suis bien disposé envers la Suisse, cela ne m’empêche pas d’être critique. Je n’oublie pas que la Suisse a trempé dans à peu près toutes les sales affaires depuis les nazis jusqu’aux Américains. Ils ont quand même signé un accord de renoncement à la neutralité pour suivre les Américains en 1951. Le cosignataire était le général Montgomery. Maintenant il faut distinguer un peuple de ses gouvernements.

Il faut savoir que la Suisse est beaucoup moins indépendante qu’elle ne le pense. Elle était l’un des derniers pays à indexer sa monnaie sur les réserves d’or. Le FMI a imposé l’abandon de cela à la Suisse (1er janvier

2000). Elle obéit aux ordres.

Ce dossier médical du patient sera hébergé où et par qui ? Je crains que si la Suisse oblige les patients à l'utiliser ce soit démocratiquement grave. Les données médicales sont extrêmement sensibles.

On a pu constater ces dernières années que l'importance de les protéger était toute relative…

En effet. Certaines ont été utilisées à des fins de surveillance policière. Orwell n'avait même pas pensé à ça.

Sommes-nous écoutés en permanence ? J'ai remarqué qu'il m'arrivait d'avoir des conversations orales sur certains sujets que je retrouvais ensuite sur mon écran, alors même que je n'avais rien recherché en ce sens.

Vu votre activité, je pense que cela doit allumer quelques lumières rouges dans certains pays et certaines agences. Je pense que vous faites partie des personnes ciblées. Mais ce que vous décrivez -là, c'est la fonction Siri d'assistant vocal. Ces assistants écoutent en permanence.

Il y a eu une inflexion très, très nette des cours de bourse d'Apple lorsqu'il a annoncé Siri. Pourquoi ? Avant les assistants vocaux, on ne pouvait capter les données des gens que lorsqu'ils téléphonaient ou étaient devant un ordinateur. C'est bête. Et si on inventait un système qui les écoutait en permanence ?

(Re) lire notre interview de Solange Ghernaouti : *« La surveillance de masse est déjà en place »*

En réalité c'est pire que ça : intéressez-vous à ce qu'on appelle les balises ultrason (voir https://hackaday.com/2017/05/04/ultrasonic-tracking-beacons/). Quand on regarde la télé et qu'il y a une pub. Ensuite on va sur sa tablette, qui était dans la même pièce, et celle-ci propose le même contenu que celui que l'on a vu à la télé. Il faut savoir que de plus en plus de pubs intègrent ces balises ultrason qui peuvent communiquer avec un appareil comme une tablette ou un téléphone, dont la distance est de 7 mètres, qui va recevoir l'information, pour qu'on lui propose le même contenu quand il va prendre un autre environnement.

Quel était l'endroit où on pouvait parler à peu près discrètement et faire éventuellement d'autres choses ?

Les toilettes ?

Il commence effectivement à y avoir des toilettes connectées. Mais je pensais à la voiture. Les voitures ont maintenant des systèmes d'assistant vocaux. Il a été révélé récemment que des employés de Tesla avaient accès à toutes les données collectées par les Tesla et notamment des activités plutôt intimes

dans les voitures. Parce qu'elles sont bourrées de caméras et de micros (voir par exemple ICI).

Le but des GAFAM est que chaque segment de nos vies doit faire l'objet d'une captation de données : quand on dort (montres connectées) quand on est mobile et l'on fait autre chose (smartphone, voiture…)

Dans un but commercial ?

Au début oui. Mais elles fournissent ces données aux services de renseignement. Quand ceux-ci font une requête, les sociétés n'ont pas le droit d'avertir leurs clients, sous peine de condamnation.

Ces données permettent également d'influer sur le cours de l'histoire, comme on l'a vu avec le scandale Cambridge Analytica ?

Ou l'élection de Trump, effectivement. Ou les 90 députés d'extrême droite du Reichstag. À chaque fois, on sait qu'il y a eu de l'exploitation de données qui a servi à alimenter, de manière ciblée, des fake news et de faire de la manipulation d'information.

Cambridge Analytica n'a pas disparu, elle a juste changé de nom. Elle s'appelle Emerdata maintenant. Et depuis, d'autres sociétés se sont créées. L'influence politique des sociétés s'est développée et plus aucun processus électoral désormais ne sera pas souillé par ce genre de choses, à des degrés divers.

Ce sont donc les GAFAM qui dirigent le monde ?

Les grandes sociétés, qu'elles soient américaines ou chinoises, oui.

Désormais, beaucoup de gens décident de quitter WhatsApp pour Signal ou Telegram. D'utiliser Protonmail plutôt que Gmail et de fuir Zoom pour Framatalk, par exemple. Est-ce que cela change vraiment quelque chose ou pas ?

Il vaut mieux utiliser Signal que Telegram, déjà. Mais oui, ce n'est pas inutile. Pour deux raisons : les systèmes sont ouverts et sont très bien documentés. J'ai analysé et fait analyser Protonmail, par exemple, par mes étudiants et ils ont plongé le nez dans les algorithmes.

Deuxièmement, les gens ont besoin de sécurité. Les entreprises, ou une activité comme la vôtre, les avocats et les journalistes sont des professions à risques et pas qu'en Iran. Dans des pays bien démocratiques, un journaliste d'investigation qui veut vraiment faire son travail peut se mettre en danger. Il y a quand même des journalistes qui ont été tués à Malte. Il y a un vrai besoin de sécurité.

Ces technologies sont crédibles, car elles offrent des outils qui, quand on

sait bien les utiliser, peuvent effectivement nous garantir que, même en cas de duplicité, on serait protégés. Cela implique toutefois que les gens soient éduqués et informés.

Qu'ils soient soucieux du problème aussi. J'entends beaucoup l'argument « Je n'ai rien à cacher » lorsque l'on évoque la surveillance de masse.

Est-ce que l'on a envie que notre banquier à qui on va demander un prêt soit au courant de notre début de cancer ? Snowden disait : « n*e pas se protéger parce qu'on n'a rien à cacher revient à dire que la liberté d'expression n'a aucun sens parce qu'on n'a rien à dire* ». C'est une phrase admirable qui vaut toutes les explications.

Il y a deux choses qui sont constitutives de la vraie liberté : la propriété – or, les GAFAM veulent remplacer la propriété par l'usage – et la vie privée, avec ses corollaires le droit à l'oubli, à l'erreur, etc.

Comment a-t-on progressé en tant qu'humain ? C'est par nos erreurs. Par nos échecs plus que par nos réussites. Dans une dictature de la transparence, on pourrait sortir à tout moment une photo vieille d'il y a 20 ans, sortie de son contexte, qui permettrait à n'importe qui de juger. La vie privée est constitutive de la liberté. Il y a des moments où on a besoin de se retrouver avec soi-même. C'est très, très important.

Pour terminer, parlez-nous un peu de Crypto AG, puisque vous en savez plus que nous.

Je ne peux pas tout dire, parce que j'ai travaillé dessus et j'ai eu accès aux *backdoors* et aux algorithmes. Mais allons-y : à la fin de la guerre, la Suisse a opté pour une neutralité et les pays anglo-saxons avaient compris que celui qui contrôle la crypto contrôlera tout. Il y avait très peu de sociétés qui vendaient des systèmes de cryptographie (les machines à chiffrer) : Crypto AG, Siemens, Ericsson, Transvertex, Racal… Entre 120 et 130 pays en ont acheté, pour leurs besoins gouvernementaux, diplomatiques, des machines à chiffrer suisses en pensant être super bien protégés.

Parmi les clients de Crypto AG, il y avait l'Iran. En 1995, Hans Bühler, l'un des top VRP de Crypto AG, se rend en Iran et il est retenu prisonnier pendant neuf mois. Durée suffisante pour le faire accoucher d'un certain nombre de choses.

Hans Bühler[3] a révélé que toutes les machines vendues à ces 130 pays contenaient des *backdoors*, donc des portes dérobées qui permettaient le décryptement plus facile. Et que les Américains revendaient les informations. Quand l'Iran a découvert que les informations étaient données gratuitement aux Israéliens dans le cadre du conflit Iran/Irak, les Iraniens ont fait des bonds. Quand le Pérou a découvert que, lors des négociations commerciales sur les accords de libre-échange avec les États-Unis, ces derniers étaient au courant de tout à l'avance, cela a été une catastrophe pour le Pérou. Les cas sont très nombreux et tous ne sont pas encore publics.

> *« Les États ne tolèrent pas qu'il puisse y avoir des moyens de sécurisation réels »*

Crypto AG, mais aussi d'autres sociétés européennes, a ouvertement collaboré avec les Américains pour affaiblir toute la crypto mondiale de la plupart des pays et je peux le confirmer, car j'ai travaillé dessus.

Ce qu'on a vu à l'époque avec Crypto AG, on le voit maintenant avec le mécanisme des zero-day. Ces failles connues et volontairement non corrigées. Les États ne tolèrent pas qu'il puisse y avoir des moyens de sécurisation réels. On fait donc des affaiblissements, on met des *backdoors* ou on tarde à corriger des failles. C'est ce que l'on appelle pudiquement le « control export » (désormais encadré par les accords de Wassenaar). Crypto AG s'est fait prendre, mais ce n'est pas la seule.

Il faut bien comprendre une chose : les États sont confrontés à un dilemme qui est d'un côté de protéger les citoyens et d'autre part que ceux-ci ne puissent pas se protéger de l'État. Il doit pouvoir attaquer et contrôler en permanence. C'est compréhensible quand il s'agit de lutter contre le banditisme et autre, mais on a bien vu que nous sommes dans une société de surveillance globale. Quand les valeurs démocratiques sont affaiblies, la tentation est alors forte de passer à une surveillance globale plus ou moins forte… même dans les pays européens.

Tout cela est très encourageant…

Soit on perd notre esprit citoyen et il n'y a plus d'espoir. Mais je pense qu'il faut rééduquer les gens et développer leur sens critique. Il faut se réapproprier une certaine hygiène de la sécurité et revenir à une certaine frugalité numérique.

Dans le monde virtuel, on a encore plus besoin de sécurité que dans le monde réel. Mais les gens semblent l'avoir oublié.

---

1 https://www.nextinpact.com/article/71104/la-commission-europeenne-veut-surveiller-integralite-web-mails-et-messageries-chiffrees

2 Voir https://www.cnil.fr/fr/transferts-de-donnees-vers-les-etats-unis-la-commission-europeenne-adopte-une-nouvelle-decision. On a fait toute une analyse là-dessus.

3 https://www.neuer-weg.com/node/9794 j'ai fait une traduction et une analyse

du livre