Face aux pratiques de la NSA, l'Allemagne passe à l'action et met fin à ses contrats avec Verizon… quid de la France ?

Suite aux révélations d'Edward Snowden, l'Allemagne a décidé de ne plus travailler avec l'opérateur américain Verizon qui fournit une partie des réseaux de télécommunications utilisés pour interconnecter les administrations fédérales.

Avec Fabrice Epelboin

Atlantico : Le gouvernement Allemand a décidé de ne pas renouveler son contrat avec l'opérateur américain Verizon suite aux révélation des écoutes de plusieurs membres du gouvernement allemand, dont Angela Merkel. Comment la confidentialité est-elle gérée en France ? Sommes-nous dépendants d'opérateurs étrangers, et plus particulièrement américains ?

Fabrice Epelboin : Commençons par le commencement. Internet, et par extension l'essentiel de ce qui constitue les réseaux de communication, se base sur un concept de "réseau de réseaux" (littéralement inter-net). Si vous communiquez avec quelqu'un d'autre, les signaux que vous envoyez et recevez vont emprunter une route (des routes, pour être précis) qui vont traverser plusieurs réseaux. Certains seront sous écoute (comme le cas d'Orange, c'est ce qu'a "révélé" *Le Monde* il y a quelques mois), d'autres non. Certains sont écoutés par la NSA, d'autres par le GCHQ, d'autres encore par la DCRI ou la DGSE, ce qui importe peu vu que tout ce petit monde collabore.

Nous sommes dépendant de cette infrastructure, et il est parfaitement illusoire de viser à une quelconque souveraineté en la matière. Quand vous vous connectez à Facebook, même en empruntant un réseau qui à l'origine appartient à Free ou Orange, vous passerez à un moment ou à un autre sur un réseau américain. C'est comme ça. **La décision Allemande tient plus de la sanction que de la protection.**

Le gouvernement fédéral allemand ne fera plus faire appel à des prestataires étrangers pour assurer ses communications, et mettra en place une architecture unifiée et gérée par l'opérateur Deutsch Telecom. Comment sont organisées les communications sensibles en France ?

Attendons de vois comment les Allemand mènent à bien pareil projet.**A défaut d'être efficace, il sera au minimum profitable à l'économie locale. c'est déjà ça. Ne pas faire intervenir de prestataires étranger sur des infrastructures souveraines est en**

effet une bonne idée.

Si on appliquait ça en France, on construirait un “cloud souverain” avec des prestataires français... Comme SFR... Jusqu’au jour où ceux-ci seraient rachetés par un Numericable qui compte parmi ses plus gros actionnaire un fond comme Carlyle, avec des gens comme Georges Bush au conseil d’administration. Et là, on se dirait que... Ha. Zut. Il y a comme un problème d’approche. **Se pourrait-il que dans un monde globalisé tout cela n’ai pas le moindre sens ? Se pourrait-il que nous ne soyons pas du tout en mesure de vivre en autarcie d’un point de vue technologique ?** Flute alors. Soit c’est ça, soit quelqu’un, quelque part, se fiche de la gueule du monde (probablement au gouvernement, ce ne serait pas une première).

En France, comme ailleurs, les communications sensibles sont chiffrées.**A partir de là, peu importe qu’elles passent sur des réseaux étrangers, l’important est que les étrangers en question ne soient pas en mesure des les déchiffrer.** C’est une problématique vieille comme l’informatique. L’ordinateur moderne (electronique) a précisément été inventé pour déchiffrer les communications allemandes durant la seconde guerre mondiale. L’ordinateur de demain (quantique) sera (ou a été) inventé pour déchiffer. C’est une dynamique en terme d’innovation assez efficace et qui a fait ses preuves.

Les “étrangers” sont-il en mesure de déchiffrer les “communications sensibles” françaises ? C’est bien possible. Ce n’est pas bien clair. Ce qui est certain, c’est que la NSA (et les autres agences) font des efforts considérables pour que cela soit possible, soit en mettant au point des machines capables de le faire, soit en sabotant à la base les systèmes qui permettent de chiffrer les communications.

Un an après le scandale de la NSA, qui a aussi touché la France (qu'il s'agisse de hauts diplomates ou de membres du gouvernement), quelles ont été les mesures prises par le gouvernement pour protéger nos communications et nos données sensibles ?

Je ne vais pas vous balancer des noms, mais j’ai à de nombreuses reprises échangé avec du personnel diplomatique (pas forcément français) ou des hauts fonctionnaires en charge d’intérêts stratégiques pour la France qui utilisaient des adresses Hotmail ou Gmail. **Comme souvent, comme on dit chez les hackers, le problème est entre le clavier et la chaise.**

Autre exemple comique qui montreà quel point le problème est profond : faites une recherche “avancée” sur Google, en lui demandant de retrouver des documents de type PDF portant la mention “confidentiel” et en limitant la recherche aux sites gouvernementaux français, vous allez être surpris. Si, si, Google est parfaitement capable de faire ce genre de requète. Il suffit de savoir l’utiliser. Vous voulez du document sensible ? Vous allez être servi. Allez, je vous aide : http://bit.ly/1lkZsfk

Faites attention tout de même, j’ai un collègue journaliste qui s’est retrouvé devant les tribunaux pour avoir utilisé Google de la sorte.

On a vu notamment l'arrivée de téléphones portables ultra-sécurisés destinés à être utilisés par les décideurs politiques et le corps diplomatique. Pourtant, on voit souvent dans la presse des membres du gouvernement utilisant des téléphones courants. Cette insouciance est-elle justifiée ?

J’adore l’idée de confier la confidentialité de mes échanges à un acteur des technologie par ailleurs impliqué jusqu’au cou dans la surveillance. C’est tellement comique que ça laisse sans voix. On se demande tout de même qui peut être assez stupide pour souscrire conceptuellement à une telle solution. Le dernier abruti qui s’est fait avoir s’appelait Mouammar Kadhafi, c’était l’objet de la première transaction dans les contrats connus sous le nom de “l’affaire Takieddine”, avec une entreprise portant le nom d’i2e, plus connue sous le nom d’Amesys, qui est devenue ce qui s’appelle aujourd’hui Bull. Mouammar a amèrement regretté par la suite cette erreur de jugement.

Les politiques qui utilisent des technologies non sécurisées sont bien évidemment sous écoute- ils font même parti des privilégiés à ne pas être écoutés que par des machines, mais également par de vrais êtres humains, et probablement par une multitude d’agences de différents pays, à commencer par leurs propres agences de renseignement nationales, et potentiellement, depuis le vote de la Loi de Programmation Militaire en décembre dernier, du Premier ministre et de l’Elysée.

Le problème est qu’ils ne comprennent rien aux technologies courantes qu’ils utilisent tous les jours.Si vous êtes invité à un diner de cons et que vous ne savez pas qui est le con à table, c’est que c’est vous. C’est aussi bête que ça.

Il n’existe pas de solutions simples pour sécuriser vos communications. Il faut avant tout comprendre ce que l’on fait. Il faut par exemple comprendre qu’à partir du moment où vous allumez votre téléphone sans fil, les antennes relais vous localisent - c’est leur fonction de base, elles ont besoin de cela pour établir une communication. Ces antennes fonctionnant - pour la plupart - sur des technologies chinoises, on peut imaginer que les chinois vous localisent (pourquoi pas), et comme elle sont connectées au réseau de votre opérateur, celui ci aussi vous localise. Toutes ces opérations laissent des traces, qui peuvent (ou pas) être utilisées pour vous pister, c’est à dire vous localiser mais pas dans le seul but de faire passer votre conversation dans les tuyaux. Dans le meilleur des cas, ces traces seront conservées au cas où elles puissent s’avérer utiles par la suite. Cette simple opération se révèle assez complexe, en réalité, et il en est de même pour à peu près tous les usages de technologies de nos jours. Tant que tout cela reste obscur, c’est vous le con à table.

Que reste-t-il à faire ?

I**l suffit juste d’apprendre à lire, et eventuellement à écrire.**Nous faisons face aujourd’hui à une nouvelle forme d’illetrisme, l’illetrisme technologique. Celui ci est facilité par l’extreme simplicité apparente des technologies du quotidien, qui cachent une grande

complexité technique. Tant que vous n'abordez pas la complexité, vous êtes un illétré, et vous ne pouvez prétendre à maitriser votre destin dans un monde de plus en plus technologique.

La situation de l'homme de la rue au XVe siècle était similaire. Ne sachant pas lire, il n'avait pour seul recours, s'il voulait comprendre le monde qui l'entoure, de s'adresser à l'église, qui lui fournissait des illustrations simples (sous forme de vitraux et de statuaires), un intermédiaire avec le savoir (un prètre), et une vision assez limpide lui donnant réponse à tout. Ainsi, la terre avait été créée en sept jours par Dieu. Point barre.

Cette explication suffisait à la plupart des hommes au XVe siècle, tout comme la compréhension des technologies très approximative suffit aujourd'hui à la plupart des hommes du XXIe.

La vrai question aujourd'hui est de savoir si cette explication vous suffit. Voulez vous continuer de confondre la maitrise d'une interface utilisateur et la compréhension des technologies sous jacentes ? Etes vous conscient des sacrifices en termes de libertés lié à cette ignorance ? L'homme du XVe siècle a fini par réaliser qu'il vivait dans un système où les richesses et le pouvoir étaient dans les mains exclusives du clergé et de l'aristocratie, il a appris a lire, il s'est mis a fantasmer sur un monde possible - le siècle des Lumières - puis il a changé la façon dont le pouvoir se distribuait - la révolution.

Bien sûr, nous sommes au XXIe siècle, et cette métaphore a ses limites. Aujourd'hui, tout va bien plus vite.