Tous les secrets pour éviter de se faire écouter par la NSA

Les révélations sur le programme Prism ont lancé une nouvelle mode : les cryptoparties. Ces ateliers permettent d'apprendre à protéger ses données et ses communications.

Avec Jérémie Zimmermann

Atlantico : Des « cryptoparties » s'organisent en Allemagne. Derrière ce nom barbare, se cachent des sessions de formation destinées à enseigner à ceux qui le désirent les techniques d'encodage pour protéger leurs données. L'idée connaît en effet un véritable boom suite aux révélations sur le programme PRISM. Les organisateurs invoquent l'incapacité de l'Etat à protéger les citoyens, revient-il à chacun de prendre ses responsabilités pour se protéger ?

Jérémie Zimmermann : Ces cryptoparties s'inscrivent, plutôt que dans un mouvement, dans une mouvance de plus en plus large de récupération par les citoyens de la maitrise du web, de la confidentialité de leurs données et des outils de communication en général. A cette même logique appartiennent notamment les *hackers space* qui se développent dans toutes les capitales et les villes secondaires et qui permettent de mutualiser un certain nombre d'équipements comme les imprimantes 3D ; citons également la mouvance des *makers* dont le mot d'ordre est le partage qu'il s'agisse de techniques de piratage ou de recettes de cuisine.

L'affaire PRISM nous a clairement montré que la surveillance par les entreprises qui gèrent les données et la surveillance d'Etat ne sont qu'une seule et même chose ou presque. Et cela nous a surtout montré que la sécurité ne peut être assurée que par l'utilisateur lui-même. **A partir du moment où l'on s'en remet à un tiers, professionnel ou étatique, on s'expose à ce que la sécurité de nos données soit remise en cause**.

Il faudrait pour faire confiance à l'Etat que soit établi un cadre législatif sans compromis avec les libertés fondamentales et donc qui interdirait la surveillance massive disproportionnée et imposerait des sanctions aux entreprises qui abusent de l'usage des données. Pour l'instant, force est de constater que nous en sommes loin. Nous pourrions aussi attendre de l'Etat des politiques industrielles visant à développer la diffusion et l'usage des outils de protection des données et des communications personnelles par exemple autour de l'utilisation de logiciels libres et de la généralisation de la cryptographie. Là encore, il n'en est rien et tout passe par des contrats gigantesques signés avec Microsoft plutôt que d'aider l'industrie informatique locale.

Les cryptoparties prônent l'encodage, et plus précisément le chiffrement, comme moyen de protection de ses mails. En quoi cela consiste-t-il ?

Encoder signifie transformer une information en un code, pas nécessairement chiffré. Si c'est le cas, comme souvent dans ces cryptoparties, il s'agit de chiffrement qui est lui-même une sorte d'encodage. **Le chiffrement consiste à utilise les mathématiques pour embrouiller un message à l'aide d'une clé et donc le rendre lisible uniquement avec cette clé**. Clé que votre correspondant est censé posséder. Cela implique donc une sorte de discipline, de gymnastique qu'est la gestion des clés, leur entretien, leur renouvellement etc. Ce sont de petites habitudes qu'il faut prendre et de petites techniques qu'il faut connaître. C'est à très peu de choses près similaire à la gestion de nos différentes "clés physiques", dans laquelle il faut se souvenir que telle ou telle clé correspond à telle ou telle serrure. Ou encore que cette serrure possède deux clés, que si une est perdue ce n'est pas grave mais que l'autre doit être protégée etc.

La cryptographie informatique n'est donc finalement pas si éloignée de ce qui s'est toujours fait pour cacher des informations, comme le firent par exemple en France les templiers ?

Cela remonte même très loin, et l'Histoire du cryptage est remplie d'anecdotes surprenantes. Sous l'Empire romain, on rasait les esclaves, on leur tatouait un code sur les zones pileuses et on les envoyait traverser les lignes ennemies ensuite. Le parallèle historique a cela d'intéressant qu'il montre bien que **jusque très récemment la cryptographie était réservée aux questions militaires**. L'un des exemples les plus célèbres de l'utilisation de cette technique sont les machines Enigma utilisées pour chiffrer les communications du IIIème Reich et dont le cassage du code par les Britanniques a donné un avantage décisif aux Alliés. Aujourd'hui, l'avènement du micro-ordinateur et plus largement la généralisation de l'accès à une grande puissance de calcul ont fait de la cryptographie un outil pour tout le monde alors qu'elle fut longtemps considérée comme une arme de guerre.

La cryptographie suffit-elle à se protéger au quotidien ? D'autres techniques - comme utiliser des moteurs de recherche moins connus que Google et Yahoo – sont-elles efficaces ?

Seule la cryptographie permet aujourd'hui de protéger efficacement ses données personnelles. En effet, il faut savoir que les protocoles du Net sont très anciens, ils remontent à une époque à laquelle la cryptographie n'était pas accessible à tous et ne sont donc pas protégés comme les protocoles d'envois de mails qui ne sont pas chiffrés. **Votre mail n'est donc qu'une carte postale qui peut être lue en chemin**. Ensuite, si un gouvernement fait de la surveillance massive, comme de l'écoute de fibres optiques par exemple, que vous utilisiez un site connu ou pas vous n'êtes à l'abri d'aucune surveillance.

S'il était possible de casser les outils de cryptographie les plus utilisés aujourd'hui, il est probable que nous le saurions, cependant ne faisons pas d'angélisme : la capacité des gouvernements à le faire est plus grande que ce qu'ils veulent bien en dire. Cependant, cela nécessite des efforts et du temps très importants, et **si tout le monde cryptait ses communications, nous serions tous mieux protégés, aussi bien par le cryptage en lui-même que par l'énergie supplémentaire que devraient déployer les gouvernements pour nous surveiller**. Pourtant, lire un contenu ne nécessite par forcément de casser une cryptographie, il suffit d'obtenir le code. Ce qui est bien plus facile, et cela sans aller jusqu'à la technique ancestrale qui consiste à taper sur les rotules de votre cible jusqu'à ce qu'elle vous livre le code. Les services de renseignements ou autres, utilisent des caméras mais aussi l'analyse du bruit des touches qui est vulnérable aux attaques statistiques pour trouver le code recherché. Enfin, de nombreux autres paramètres de sécurité peuvent être piratés et donc rendre la cryptographie superflue !

La cryptographie est donc une techniques très efficace mais elle n'est pas l'alpha et l'oméga - utilisée sans une gestion minutieuse des autres paramètres de sécurité informatique elle est en partie inutile. Précisons tout de même que de manière générale dans la sécurité, et donc dans la sécurité informatique, la protection 100% n'existe pas. La question de fond est donc de savoir contre qui on se bat, se protéger d'un mari jaloux n'est pas la même chose que d'être ciblé par une agence de sécurité américaine qui vous accuse de terrorisme.

Propos recueillis par Jean-Baptiste Bonaventure