À bâbord !
Revue sociale et politique

Esquiver la surveillance numérique

Antoine Beaupré

Numéro 83, mars 2020

Perturbations à prévoir

URI : https://id.erudit.org/iderudit/94019ac

Aller au sommaire du numéro

Éditeur(s)

Revue À bâbord !

ISSN

1710-209X (imprimé)
1710-2103 (numérique)

Découvrir la revue

Citer cet article

Beaupré, A. (2020). Esquiver la surveillance numérique. *À bâbord !*, (83), 50–50.

ESQUIVER LA SURVEILLANCE NUMÉRIQUE

Antoine Beaupré*

Je répond ici à trois questions : quels sont les meilleurs moyens pour s'assurer qu'une action ne soit pas découverte avant sa mise en œuvre ? Y a-t-il des outils qui permettent de limiter la surveillance en ligne et si oui, lesquels ? Comment limiter les pistes laissées derrière soi en cas de risque de poursuite au criminel pour soi ou pour les allié·e·s ?

Les manières de s'assurer qu'une action ne soit pas découverte avant sa mise en œuvre varient selon les moyens d'action. Une vigile pacifique devant une ambassade va requérir moins de confidentialité que le blocage d'un pont. Garder toute action d'envergure secrète est un problème extrêmement difficile, peu importe les moyens technologiques. Comme le dit l'adage attribué à Benjamin Franklin, *«trois personnes peuvent garder un secret, si deux d'entre elles sont mortes»*. Fondamentalement, on «potine», on jase, on en dit trop. La première chose à faire est de lutter contre ce penchant et établir une «sécurité opérationnelle» dans l'organisation. On partage l'information seulement avec les personnes qui ont besoin de la connaître. On segmente l'organisation en petits groupes.

La même chose se produit en ligne. Si tout le monde s'organise sur le même groupe Facebook ouvert, il y a plus de risques d'infiltration que si on opère sur des petits groupes Signal ou WhatsApp. Mais à l'inverse, c'est plus difficile de rejoindre les gens hors des plateformes de masse, alors c'est toujours une question de compromis entre la confidentialité et la diffusion de l'opération.

Comme Snowden nous l'a enseigné, le chiffrement fonctionne, même contre les plus hauts niveaux de surveillance tels que la NSA. Si on veut limiter la surveillance en ligne, il faut donc privilégier des plateformes chiffrées comme Signal ou WhatsApp ou d'autres, pour ceux et celles qui font confiance au serveur central, telles que Messenger ou Facebook.

Plus généralement, des outils comme le navigateur Tor («Tor Browser») sont très efficaces pour cacher d'où on vient sur Internet. Ils permettent aussi, dans une certaine mesure, d'empêcher que la surveillance puisse découvrir où et par qui est hébergé un serveur… Des outils comme OnionShare utilisent également Tor pour partager des fichiers et des sites web de la même façon.

Je recommande également d'installer un bloqueur de pub (uBlock origin) et possiblement de JavaScript (NoScript, activé par défaut dans Tor Browser ou uMatrix) pour protéger la sécurité de son ordinateur en général. Et bien sûr, les avis habituels sur l'hygiène sont de mise: utiliser un gestionnaire de mot de passe avec un (un seul !) long mot de passe formé d'au minimum six mots, ne pas réutiliser les mots de passe, faire preuve de prudence avec l'ouverture des pièces jointes dans les courriels en s'assurant de leur provenance et en les ouvrant en ligne plutôt que sur l'ordinateur, etc.

Le risque avec les «outils» est qu'ils deviennent une barrière à l'inclusion qui réserve la participation aux seules personnes qui savent les utiliser. Il faut aussi faire attention avec ces outils parce qu'ils peuvent donner un faux sentiment de sécurité et exposer davantage les personnes qui cessent de présumer qu'elles sont possiblement sous surveillance (ou surveillées). Même les expert·e·s font parfois des erreurs, et c'est extrêmement difficile de dissimuler des projets lorsqu'on est déjà sous surveillance.

Des systèmes comme «TAILS» peuvent aider à limiter les pistes laissées derrière soi. Il s'agit d'un système d'exploitation «jetable» qu'on installe sur une clé USB, et qui ne garde aucune trace de l'activité sur l'ordinateur. Ce système est également basé sur Tor.

En général, il faut limiter au maximum l'information qu'on génère. Soyez conscients des traces que vous laissez dans vos courriels, dans l'historique de navigation, dans vos discussions en ligne, tout ceci peut être sujet à un mandat de perquisition. Le chiffrement des disques par VeraCrypt (Windows, Linux) ou FileVault (Mac) peut protéger vos données d'une attaque, pourvu que votre mot de passe soit solide. Il est à noter que, en cas de risque de poursuite criminelle, la Cour pourrait vous forcer à divulguer votre mot de passe, car les protections légales à ce niveau ne sont pas encore tout à fait claires.

Ne pas écrire ou dire quelque chose qui pourrait être retenu contre nous plus tard est la seule véritable protection, mais cela limite grandement la liberté d'action et la solidarité. Il faut avoir conscience du risque et le défi est de savoir maximiser la sécurité tout en conservant le maximum d'efficacité dans la communication essentielle à l'action. ab!

* Administrateur de système, projet de navigateur Tor.