Obfuscation; A User's Guide for Privacy and Protest

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 mai 2020

https://www.bortzmeyer.org/obfuscation.html

Auteur(s) : Finn Brunton, Helen Nissenbaum
ISBN n°978-0-262-02973-5
Éditeur : MIT Press
Publié en 2015

Beaucoup d'efforts sont aujourd'hui dépensés pour protéger la vie privée sur l'Internet. En effet, le déploiement des réseaux informatiques a permis une extension considérable de la surveillance, privée comme étatique. Il est donc logique que des informaticiens cherchent à développer des moyens techniques pour gêner cette surveillance, moyens dont le plus connu est le chiffrement. Mais aucun moyen technique ne résout tous les problèmes à lui seul. Il faut donc développer une **boîte à outils** de techniques pour limiter la surveillance. Ce court livre <https://mitpress.mit.edu/books/obfuscation> est consacré à un de ces outils : le brouillage ("*obfuscation*" en anglais). Le principe est simple : le meilleur endroit pour cacher un arbre est au milieu d'une forêt.

Le principe du brouillage est en effet simple : introduire de fausses informations parmi lesquelles les vraies seront difficiles à trouver. Cette technique est surtout intéresssante quand on ne peut pas se dissimuler complètement. Par exemple, le logiciel TrackMeNot <https://trackmenot.io/> (dont une des développeuses est une des auteures du livre) envoie des recherches aléatoires aux moteurs de recherche. On ne peut pas empêcher ces moteurs de recherche de connaître nos centres d'intérêt, puisqu'il faut bien leur envoyer la question. Le chiffrement n'aide pas ici, puisque, s'il peut protéger la question sur le trajet, il s'arrête au serveur à l'autre extrémité. Mais on peut noyer ces serveurs sous d'autres requêtes, qu'ils ne pourront pas distinguer des vraies, brouillant ainsi l'image qu'ils se font de l'utilisateur.

À ma connaissance, il n'existe pas de traduction idéale du terme anglais "*obfuscation*", qui est le titre de ce livre. Wikipédia propose offuscation, ce qui me fait plutôt penser à « s'offusquer <https://fr.wiktionary.org/wiki/s%E2%80%99offusquer#fr> ». À propos de français, notez qu'il existe une traduction de ce livre, « Obfuscation ; La vie privée, mode d'emploi <https://cfeditions.com/obfuscation/> » (avec préface de Laurent Chemla), chez C&F Éditions, mais je n'ai personnellement lu que la version originale.

Les techniciens ont facilement tendance à considérer comme technique de protection de la vie privée le seul chiffrement. Celui-ci est évidemment indispensable mais il ne protège pas dans tous les cas. Deux exemples où le chiffrement ne suffit pas sont l'analyse de trafic, et le cas des GAFA. D'abord, l'analyse de trafic. C'est une technique couramment utilisée par les surveillants lorsqu'ils n'ont pas accès au contenu des communications mais seulement aux métadonnées. Par exemple, si on sait que A appelle B, et que, dès que ça s'est produit, B appelle C, D et E, on a identifié un réseau de personnes, même si on ne sait pas ce qu'elles racontent. Et un autre cas est celui des GAFA. Si la communication avec, par exemple, Gmail, est chiffrée (le `https://` dans l'URL, qui indique que tout se passe en HTTPS, donc chiffré), cela ne protège que contre un tiers qui essaierait d'écouter la communication, mais pas contre Google lui-même, qui voit évidemment tout en clair. Bref, le chiffrement n'est pas une solution miracle. Dans ce second cas, une autre solution pourrait être de dire « n'utilisez pas ces outils du capitalisme de surveillance, n'utilisez que des services libres et sans captation des données personnelles ». À long terme, c'est en effet l'objectif. Mais à court terme, les auteurs du livre estiment (et je suis d'accord avec eux) qu'il n'est pas réaliste de demander cette « déGAFAisation individuelle <https://www.bortzmeyer.org/degafaisation-individuelle.html> ». Comme le notent les auteurs p. 59 « "*Martyrdom is rarely a productive choice in a political calculus*" ».

Le livre contient plein d'exemples de brouillage, car la technique est ancienne. Quand on ne peut pas cacher, on brouille. Des paillettes qui font croire à la défense anti-aérienne qu'il y a plein d'avions supplémentaires, au génial film de Spike Lee, "*Inside Man*" (non, je ne vais pas divulgâcher, regardez le film), les exemples ne manquent pas. Cette technique a été largement utilisée en informatique, et le livre comprend une passionnante description de l'opération Vula, où il ne fallait pas simplement dissimuler le contenu de la communication, mais également le fait qu'elle avait lieu, ce qui est bien plus difficile. Et les auteurs savent de quoi il parle puisqu'Helen Nissenbaum a également travaillé sur Ad Nauseam <https://adnauseam.io/>, un logiciel qui clique sur toutes les publicités, pour empêcher la surveillance (dont la publicité est à la fois l'un des moteurs importants et l'une des armes favorites) de savoir si les publicités sont efficaces ou pas.

Outre cette très intéressante partie sur les exemples réels (dans le monde de l'informatique, et en dehors), l'intéret du livre est une discussion détaillée de la légitimité du brouillage. Est-ce bien ou mal de « cliquer » sur les publicités, privant ainsi une profession honorable des informations sur la vie privée des utilisateurs (pardon, les pubards les appellent les « cibles »)? Les auteurs insistent que le brouillage est l'arme du faible. Les riches et les puissants peuvent se cacher, ou échapper à la surveillance, le brouillage est pour ceux et celles qui ne peuvent pas se cacher. C'est cette asymétrie qui est le principal argument en faveur de la légitimité du brouillage (p. 78).

Et le problème écologique ? Le brouillage consomme davantage de ressources, c'est sûr. La question est suffisamment sérieuse pour faire l'objet d'un traitement en détail dans le livre (p. 65), je vous laisse découvrir la discussion dans le livre.

Ceci dit, de même que le chiffrement n'est pas la seule technique à utiliser dans la lutte pour préserver sa vie privée (p. 62), de la même façon, il ne faut pas penser qu'aux solutions techniques. Ne pourrait-on pas compter sur la bonne volonté des entreprises privées, pour qu'elles arrêtent la surveillance ? (p. 60, les auteurs expliquent pourquoi ils n'y croient pas.) Et, sinon, sur les États pour arrêter cette surveillance par la loi ? (p. 61, les auteurs sont pessimistes à ce sujet.)

Enfin, le livre compte aussi d'autres discussions passionnantes, mais je vous laisse les découvrir. Bonne lecture ! (Et, après, il y a une grosse bibliographie, si vous voulez approfondir.)

`https://www.bortzmeyer.org/obfuscation.html`