# surveillance://

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 octobre 2016

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

Auteur(s) : Tristan Nitot
ISBN n°978-2-915825-65-7
Éditeur : C&F éditions
Publié en 2016

———————-

Si vous avez lu tous les articles d'Amaelle Guiton <http://www.liberation.fr/auteur/15260-amaelle-guit de bluetouff <https://reflets.info/author/bluetouff/> et d'Andréa Fradin <http://riverains.rue89.nouvelobs.com/andrea-fradin>, si vous allez à tous les Quadr'Apéro <https://wiki.laquadrature.net/Quadr%27ap%C3%A9ro> de la Quadrature du Net (en lisant un livre de Schneier dans le métro) ou, bien sûr, si vous travaillez pour Facebook ou pour la DGSI, ce livre <http://cfeditions.com/surveillance/> ne vous apprendra rien. Vous savez déjà que l'internaute ordinaire (pas le suspect de djihadisme ou de grand banditisme, non, le fameux M. Michu) est surveillé en permanence par les outils et services numériques qu'il utilise. Mais, contrairement au djihadiste ou au bandit, M. Michu ne le sait pas, ou bien il ne mesure pas exactement l'ampleur de la surveillance généralisée, ou alors il est complètement résigné, convaincu de ne rien pouvoir y faire. Le livre de Tristan Nitot <http://cfeditions.com/surveillance/> vise à informer cet internaute innocent (dans tous les sens du terme) de la surveillance dont il fait l'objet, mais aussi à proposer des pistes pour améliorer les choses et faire reculer un peu la surveillance. (La préface d'Adrienne Charmet insiste sur l'importance de marcher sur ces deux jambes, l'exposition des problèmes, et celle des solutions.)

Ce livre est très court, ce qui reflète soit la paresse de l'auteur, soit son désir d'être utile à un maximum de gens qui pourraient être découragés en voyant un énorme pavé universitaire (qui, au passage, manque, sur ce sujet). L'auteur présente d'abord la variété des techniques de surveillance existantes. Contrairement à ce que prétendent les menteurs qui affirment qu'avec le chiffrement des "*smartphones*", les policiers ne pourraient plus travailler, notre vie privée a énormément perdu avec l'arrivée de ce "*phono sapiens*". Doté de capteurs perfectionnés, il enregistre tout et transmet tout à ses maîtres (qui ne sont pas son propriétaire...). Ensuite, les GAFA comme Google récoltent une quantité faramineuse de données, que leurs techniques perfectionnées permettent d'analyser. L'auteur donne plusieurs exemples concrets et précis (avec à chaque fois l'URL permettant d'aller se renseigner davantage, souci de sérieux rare). Toute cette partie est très pédagogique. Si vous êtes le "*geek*" instruit et politisé cité au début, c'est l'ouvrage à recommander à vos proches (et aux lointains aussi) moins informés, pour qu'ils comprennent ce qui arrive aujourd'hui à tout citoyen. Et ne leur racontez pas tout, laissez-leur le plaisir de découvrir l'erreur gravissime du cochon, citée à chaque conférence de l'auteur :-)

Tristan Nitot tord aussi le cou à quelques mythes comme le « je n'ai rien à cacher ». On a tous des choses (tout à fait légales) à cacher. Personnellement, je demande aux gens qui affirment n'avoir rien à cacher « votre dernier relevé bancaire, et la liste de vos dix derniers partenaires sexuels, avec les pratiques utilisées ».

Un point important de son livre est la question du modèle économique des acteurs de l'Internet. Si Google et Facebook nous surveillent autant, ce n'est pas parce qu'ils sont des filiales de la NSA, ni parce qu'ils sont vendus au diable ou aux reptiliens. C'est parce qu'ils sont gratuits, et qu'il faut bien se financer d'une manière ou d'une autre. Exploiter les données personnelles est une méthode rentable, et largement invisible pour l'utilisateur. Elle nécessite la récolte du plus grand nombre de données personnelles possible, et il n'est donc pas exagéré de noter que « le modèle d'affaires du Web, c'est la surveillance ».

Le désir de l'auteur (et de la préfacière) de ne pas uniquement décrire l'affreuse surveillance dont nous sommes l'objet, mais également de faire preuve d'un certain optimisme en indiquant des choix qui amélioreraient les choses, va parfois un peu loin. Si je peux comprendre l'analyse mesurée que Nitot fait d'Apple (société dont il ne cache pas les défauts mais qui, en matière de surveillance, semble en effet « moins pire » que les autres), j'ai plus de mal avec l'éloge qu'il fait de la société Sen.se dont le fondateur répète partout que la vie privée n'est pas son problème car « Facebook fait pire ». C'est ainsi que le produit Mother de cette société envoie tout dans « un ordinateur de quelqu'un d'autre » et que c'est présenté comme inévitable <http://www.lesnumeriques.com/objet-connecte/mother-p18525/sen-se-mother-securite-donnees-rafi-haladjian-repond-n36875.html>.

L'auteur continue en expliquant qu'un autre Internet est possible. Car dénoncer la surveillance, c'est très bien, mais cela peut mener à la sidération : convaincu d'être surveillé de partout, et de ne pas pouvoir l'empêcher, sauf à vivre dans une grotte sans électricité, le citoyen pourrait se décourager et renoncer à son droit à la vie privée. Il est donc nécessaire de proposer des pistes d'amélioration. Plusieurs sont avancées : le logiciel libre, bien sûr, condition nécessaire (mais pas du tout suffisante), le paiement des services (« si c'est gratuit, c'est que vous n'êtes pas le client, vous êtes la marchandise »), l'autohébergement (sans cacher, comme pour les autres solutions, les extrêmes difficultés que cela pose), le chiffrement (encore une condition nécessaire mais pas suffisante)... Nitot demande aussi que les partisans d'un autre Internet s'attaquent aussi au problème difficile de faire aussi bien, voire mieux, que les GAFA en matière de vécu utilisateur.

L'auteur détaille aussi, avec beaucoup de précision, quelques mesures d'hygiène numérique qui peuvent permettre de limiter un peu les dégâts de la surveillance. Par exemple, bloquer le "*spyware*" Google Analytics, ou bien avoir son propre nom de domaine permet de ne pas dépendre d'un seul fournisseur, et d'être donc libre de le quitter si ses pratiques ne sont pas acceptables.

Notons que ces manipulations sont parfois longues, ce qui reflète le désir des maîtres de la surveillance de nous empêcher de diminuer celle-ci. Il faut ainsi neuf étapes pour configurer Twitter de manière plus respectueuse de la vie privée.

Pour une genèse du livre, par son auteur, et pour une liste exhaustive des articles qui en parlent, voir sur le Standblog <http://standblog.org/blog/pages/Surveillance>.

Déclaration de conflit d'intérêts : j'ai reçu un exemplaire gratuit de ce livre, mais il n'était pas accompagné d'une bouteille de vin, donc j'écris cet article à jeun et en toute objectivité.