



Peut-on échapper à la surveillance ordinaire ? Comprendre et agir avec Tristan Nitot

mardi 28 février 2017, par Burkinapmepmi.com

Tristan Nitot est un “vieux natif du numérique”, c’est lui qui le dit. Le 3 octobre, il publie “surveillance ://” aux éditions C&F, un livre dans lequel il analyse la surveillance ordinaire dont nous faisons l’objet, et les moyens dont nous disposons pour reprendre le contrôle de notre vie numérique.

Quelques jours après la publication de son livre, le fondateur de l’association Mozilla Europe, nous a ouvert les portes de son appartement, et parcouru avec nous les pages de son ouvrage.

Nous sommes tous sous surveillance

“Je sais ce que vous faites dans la salle de bain, pourtant vous fermez le verrou”. Même si nous pensons ne rien avoir à cacher, nous devrions tous nous sentir concernés par la surveillance.

Avec son livre, Tristan Nitot fait le pari d’expliquer les enjeux et les mécanismes de la surveillance pour que chacun puisse s’emparer des outils qui permettent de s’en libérer.

Comprendre. Comme le dit Orwell dans son intemporel - et tellement contemporain - ouvrage 1984, “la dictature s’épanouit sur le terreau de l’ignorance”. La Palisse poursuivrait en disant que, pour ne pas ignorer, il faut savoir, et pour savoir, il faut comprendre.

“C’est un protocole de surveillance qui est en train de se mettre en place au niveau de la société”

L’enjeu n’est pas mince. Pour qui n’est pas sensibilisé à la question, la découverte est surprenante : les GAFA (Google, Apple, Facebook, Amazon), mastodontes de l’internet dans les mains desquels nous concentrons nos données, nous “pillent” littéralement. Mais là où le bât blesse, c’est que nous mettons nous même nos données à leur disposition. Noms, prénoms, nombre de clics, pages vues, temps passé sur une page, contenus des mails envoyés et reçus - les pièces jointes - géolocalisation... En signant des CGU (conditions générales d’utilisation) que nous ne lisons pas, nous acceptons que nos comportements en ligne et nos données soient passés au scanner.

Dans quel but ? Nous marketer : ou plutôt, capitaliser sur nos données, rentabiliser notre potentiel monétaire. “Facebook échange vos données contre 5 euros par personne et par an souligne Tristan Nitot mais vos données peuvent être utilisées contre vous... Et à partir de là, on est mal”.

Une menace pour les libertés



La collecte de données à grande échelle par ces mastodontes de la Silicon Valley pose question : et si nos données étaient utilisées à mauvais escient ? Si leur teneur peut paraître anodine dans un contexte donné, demain, les choses pourraient changer. "Les lois sont susceptibles de changer et ce qui est interdit ou techniquement impossible aujourd'hui peut être autorisé ou techniquement possible demain". De l'utilisation commerciale de nos données à la délation, il n'y a qu'un pas, que certains ont déjà franchi. Des cas de "délation" ont déjà été possibles grâce à de la surveillance active :

En mars 2012, Facebook a dénoncé un trentenaire originaire de Floride aux autorités après qu'un logiciel permettant d'espionner les conversations privées des utilisateurs ait détecté que l'homme communiquait avec une adolescente âgée de 13 ans.

En 2014 à son tour, Google faisait arrêter un américain qui échangeait des photos à caractère pédopornographique par mail.

Ces cas ne sont pas isolés, et Tristan Nitot d'en reprendre certains dans les pages de son livre. Systématiquement, les géants de l'internet ont brisé le caractère privé des conversations de leurs utilisateurs pour en dénoncer le contenu. Un mal, pour un bien ? Si ces pratiques ne posent pas de problème aujourd'hui, parce qu'il s'agit de pédophilie, les choses peuvent changer. Ce qui hier n'était pas considéré comme un délit, ou un crime, peut l'être demain. Il suffit d'imaginer la suite...

Alors, doit-on choisir entre internet et vie privée ?

Ces perspectives donnent le vertige. Pour autant, doit-on se résigner à être surveillés, et dire adieu à nos ordinateurs et autres smartphones pour préserver un semblant de vie privée, ou inversement ? Pour Tristan Nitot, la réponse est définitivement non. Et l'objet même de son ouvrage repose justement sur un espoir, "agir". Oui, il est possible d'agir, mais pour cela, il faut être conscient des enjeux, et savoir où chercher pour trouver de bonnes alternatives aux services classiques de mail, d'agenda, de réseaux sociaux, de carte...

"La première règle d'hygiène informatique est d'utiliser des services alternatifs qui ne vous pistent pas"

La règle essentielle, pour ne pas être pisté, c'est d'utiliser des services alternatifs respectueux des données des utilisateurs. Des associations ou des collectifs en proposent un grand nombre.

Alors, dans la boîte à outils de Tristan Nitot, que trouve-t-on ?

Qwant.com, par exemple, est un substitut de Google qui ne piste pas ses utilisateurs. Pas de propositions intuitives donc, pas de publicités ciblées.

L'association Framasoft propose des services gratuits et s'engage à ne pas utiliser les données personnelles des utilisateurs. Avec son initiative "**dégooglisons internet**", Framasoft propose, pour chacun des services "privateurs de liberté", une "alternative libre, éthique, décentralisée et solidaire".

Si vous ne savez pas comment chiffrer vos messageries, tournez-vous vers les "**cryptoparty**", dont nous

avons déjà parlé dans l'Atelier.

Mais que l'on se rassérène, ce n'est pas parce que ces services n'aspirent pas nos données et donc ne nous connaissent pas, qu'ils ne sont pas performants. Au contraire, ils pourraient même être surprenants. S'ils n'étendent pas les recherches à partir de nos "affinités" ils pourraient tout justement permettre de sortir de la "bulle" dans laquelle nous évoluons sur l'internet...

Crédits image : Marie-Stéphanie Servos & CC Getty Images - Geber86
atelier.rfi.fr