



Comment je suis tombé dans l'enfer de la surveillance globalisée – et vous aussi

par [Grégoire Barbey](#)

Publié le 12 septembre 2022 12:00. Modifié le 14 septembre 2022 07:45.

Je me souviens du premier ordinateur que mes parents ont acheté. C'était au début des années 2000, j'avais dix ans et naviguer sur le web n'avait rien d'intuitif. Les téléphones portables essaïmaient, c'était l'essor du Nokia 3310. J'étais loin d'imaginer que ces outils encore balbutiants allaient devenir indispensables et s'apprêtaient à nous tendre un piège.

Deux décennies plus tard, ces technologies sont partout, plus performantes que jamais – mais moins que demain. Elles conditionnent nos vies, au travail, à la maison et dans nos relations privées.

A ses débuts, internet, en tant que source intarissable du savoir et accélérateur inouï des échanges, était perçu par les mouvements cypherpunks comme la promesse d'une émancipation de l'individu, de liberté.

Démocratisation de l'accès à la connaissance il y a eu. Sans pour autant mettre un terme aux inégalités. Mais il y a un revers à la médaille: ces outils peuvent aussi être un obstacle aux libertés individuelles. Les GAFAM ont développé un nouveau modèle économique pour tirer parti des informations que nous autres, utilisateurs, leur offrons. L'auteure américaine Shoshana Zuboff a donné un nom à ce mécanisme: [le capitalisme de surveillance](#). Aujourd'hui, la matière première de ces géants du numérique, ce sont nos données personnelles. Nous sommes devenus le produit.

Tout est surveillé, tout le temps

Contrairement à une idée très répandue, Facebook ou Google ne vendent pas nos données, mais les conservent précieusement. Ce que ces entreprises vendent aux publicitaires, c'est la promesse de connaître suffisamment bien les individus pour leur suggérer des contenus avec lesquels ils vont probablement interagir, pour finalement passer à l'achat. Pour mieux nous connaître, ces conglomérats numériques collectent et analysent tous nos comportements. Rien

de ce qui contribue à mieux nous cerner ne leur échappe, à eux et à leurs algorithmes nourris par nos précieuses informations. Dans l'unique but d'établir notre profil.

Prises individuellement, ces données peuvent paraître anodines – qui est intéressé à connaître la vitesse à laquelle je tape sur le clavier ou le nombre de mots que j'utilise en moyenne par phrase? Pourtant, lorsqu'elles sont croisées, elles en révèlent beaucoup sur mes habitudes et mes comportements. Et le nombre d'informations qui sont récoltées à mon sujet ne cesse d'augmenter. Prenons l'exemple d'[Amazon, qui a récemment annoncé le rachat d'iRobot](#), le fabricant des aspirateurs robotisés Roomba, pour 1,7 milliard de dollars. *«La valeur de ce rachat ne réside pas dans la technologie développée par iRobot, observe Steven Meyer, fondateur de l'entreprise de cybersécurité Zendata basée à Genève. Ce qui compte, ce sont les données qu'iRobot a accumulées ces dernières années et c'est sur ce capital qu'Amazon met la main.»*

Mais pourquoi faire? Colin Angle, CEO d'iRobot, [avait déjà esquissé la valeur des informations recueillies](#) par ses aspirateurs robots en 2017: *«L'avenir de la maison connectée, ce n'est pas un téléphone où vous paramétrez, un à un, chacun de vos objets connectés. Il faut que le maximum de choses soient automatisées et, pour cela, il faut que la maison ait une vision précise d'elle-même, qu'elle sache en permanence qui s'y trouve, ce qui s'y trouve et où»*. Avec un aspirateur robot qui collecte les informations spatiales de mon appartement, Amazon pourrait être en mesure de me proposer un meuble pour combler un espace vide ou peut-être même de déduire mon profil psychologique de la manière dont j'ai utilisé l'espace de mon appartement.

Une relation asymétrique

Ma relation avec Amazon et les autres géants du numérique est foncièrement asymétrique: ils en savent beaucoup plus sur moi que je n'en sais sur eux. Et cette capacité à traquer nos comportements peut avoir des applications bien plus graves qu'un ciblage publicitaire. En témoigne la polémique en cours aux Etats-Unis, où [des femmes soupçonnées d'avoir avorté commencent d'être poursuivies](#) et où Facebook a [communiqué aux autorités de poursuite du Nebraska](#) les messages d'une adolescente accusée d'avoir avorté illégalement.

Comment exercer nos libertés dans un monde où tous nos comportements sont épiés – y compris «hors-ligne», par des robots aspirateurs ou des montres connectées? De surcroît, quand cette surveillance numérique insidieuse ne fait souvent l'objet d'aucun débat public? Même dans cette Suisse qui se gausse d'être LE modèle démocratique par excellence, la discussion autour des enjeux de la numérisation de la société fait défaut. Ce constat est partagé par l'institut Edgelands, qui réalise en ce moment même [une opération à Genève et dans plusieurs villes du monde pour créer le dialogue](#) entre les autorités et la population à propos de la numérisation et provoquer le débat sur cette société de la surveillance numérique. Démarche que *Heidi.news* suivra de près dans cette Exploration que nous lançons ici aujourd'hui.

La réponse est collective

Ces questions me passionnent depuis plusieurs années, à tel point que j'ai coécrit un livre sur le sujet, intitulé *Notre si précieuse intégrité numérique*, avec l'ancien président du Parti pirate Alexis Roussel. Il y a aujourd'hui un véritable besoin de discuter de ces questions, et bien trop souvent les responsables politiques se déclarent incompetents pour traiter cette matière.

Ils se trompent lourdement: l'enjeu est ici moins technique que sociétal. Le défi, sur les questions de surveillance numérique, est de montrer à la population le revers de la médaille. Comme le souligne Steven Meyer: *«En pratique, les gens ne sont pas toujours en mesure de faire le lien entre des comportements qu'ils ont eus et qui ont généré des données et les conséquences que ça a pu avoir sur leur vie.»* Et la surveillance numérique de souvent passer inaperçue.

Pour Charles Foucault-Dumas, responsable de projet chez HestiaLabs, [une entreprise qui a développé des outils](#) pour analyser ce que les géants du numérique font de nos données personnelles, la solution passe par l'action collective: *«A l'échelle individuelle, à part fuir les réseaux sociaux et se défaire de notre smartphone, il n'y a pas grand-chose à faire. Mais collectivement, en récupérant nos données auprès de ces plateformes, comme la loi nous le permet, nous pouvons non seulement démontrer les mauvaises pratiques pour faire évoluer les règles, mais aussi inventer des alternatives qui sont au service des utilisateurs.»* Encore faut-il mesurer l'ampleur du problème. Et c'est justement toute l'ambition de cette plongée au cœur de la surveillance numérique.