Interview

Tous connectés : protégeons-nous bien nos données ?

Steven Meyer,
CEO et co-fondateur
de ZENDATA Cybersécurité

En mai 2018, l'Union européenne (UE) s'est dotée d'une nouvelle législation consacrée à la protection des données personnelles ; la RGPD (règlement général sur la protection des données). En attendant la mouture helvétique, toutes les entreprises suisses qui traitent des affaires avec des individus situés dans l'UE doivent se calquer sur le règlement européen. Ce n'est pas pour autant qu'en tant que particulier nous devons laisser la main aux industries en matière de gestion des données. En adoptant quelques gestes simples, nous pouvons protéger et limiter ce qui peut être récolté sur nous au travers de nos comportements en ligne. Steven Meyer, expert en cybersécurité chez *ZENDATA* à Genève, nous donne ses recommandations.

Pouvez-vous nous décrire le chemin parcouru par nos données sur la toile ?

Tout d'abord, il existe deux types de données : celles que l'on partage délibérément comme, par exemple, sur les réseaux sociaux ou dans un formulaire de commande en ligne, et celles qui sont inférées par notre activité sur internet, par l'utilisation d'applications sur notre smartphone ou de nos divers objets connectés. Il faut savoir qu'avec une dizaine de mentions j'aime sur Facebook, le réseau peut déjà déterminer une partie de votre profil d'utilisateur, comme votre confession ou votre orientation sexuelle. Vous n'avez même pas besoin d'écrire votre biographie sur votre profil, vos actions virtuelles parlent pour vous. Lorsque vous interagissez sur internet, vous produisez des données qui vont circuler parfois d'un bout à l'autre de la planète, en passant par des câbles, des serveurs intermédiaires, des fournisseurs d'accès détenus par divers organismes publics et privés. Tous ces intermédiaires ont possiblement accès aux données que vous avez produites car vous êtes passés par leurs territoires.

« Sans tomber dans la paranoïa, nous devons savoir que, plus nombreuses sont les données récoltées sur nous, plus des modifications sociétales importantes pourraient surgir. »

Quel est l'intérêt de protéger nos données en tant que particuliers ? N'est-ce-pas plutôt l'affaire des personnalités, des entreprises ou des services étatiques ?

Même si l'on n'est qu'un particulier sans exposition médiatique, il est important de se pencher sur la façon dont nous utilisons internet et les différents objets connectés à notre disposition. Diverses entreprises dont vous ignorez l'identité récoltent des informations sur vous et votre famille. Elles sont d'abord monétisées et utilisées par les publicitaires. Mais elles peuvent aussi être exploitées à des fins de statistiques. Dans un futur proche, les assurances maladies pourraient, par exemple, décider d'augmenter leurs primes dans certaines régions si elles s'aperçoivent que des maladies qui nécessitent des soins onéreux y sont plus nombreuses. Cela casserait la logique de solidarité. Et ce n'est qu'un exemple parmi beaucoup. Sans tomber dans la paranoïa, nous devons savoir que, plus nombreuses sont les données récoltées sur nous, plus des modifications sociétales importantes pourraient surgir.

Les solutions alternatives aux géants du web, les GAFAM[1] sont-elles vraiment sécuritaires et plus éthiques ? Pouvez-vous nous en citer quelques-unes qui ont fait leurs preuves ?

Il existe pratiquement pour chaque géant du web une alternative plus sûre en matière de vie privée et sans publicités. Parmi elles, je peux citer *DuckDuckGo* comme alternative à *Google* ou *Diaspora* pour *Facebook*. Mais je ne suis pas encore convaincu par leur efficacité. Ces alternatives ont pour l'instant un succès moyen. Ce sont des outils moins rapides, moins efficaces et ils ne sont pas reliés au confort de tout l'écosystème mis en place par les géants. Les utilisateurs de ces alternatives finissent souvent par abandonner et retourner au confort offert par les GAFAM , même en sachant que c'est en échange de leurs données personnelles.

[1] Google,Amazon, Facebook,Apple,Microsoft

« Si c'est gratuit, c'est que je suis le produit. » Finalement, nos données sont un moyen de paiement n'est-ce-pas ? Est-ce qu'à l'avenir nous pourrons choisir de payer autrement qu'avec notre vie privée ?

Il est assez compliqué de chiffrer une donnée. Si l'on ne souhaite pas courir le risque que des entreprises revendent nos données sans nous consulter, il faut effectivement payer. Acheter des licences pour utiliser logiciels ou des services en ligne plutôt que de prendre ceux proposés gratuitement. Le scandale généré par l'anti-virus gratuit *Avast* est un exemple des risques encourus avec les services gratuits. Les données des utilisateurs ont été revendues à des tiers sans leur autorisation. Si vous décidez d'utiliser un produit gratuit, dites-vous bien qu'il faudra que l'entreprise se rémunère d'une manière ou d'une autre pour continuer d'exister. Il y a la publicité bien sûr, mais beaucoup d'internautes utilisent *ADblock*, qui sert aussi à se protéger des virus pouvant être transmis par des pubs.

Pouvez-vous résumer, en quelques points, les réflexes essentiels à avoir pour garantir que les données que nous renseignons sur internet soient bien protégées ?

- Se renseigner sur le site sur lequel nous naviguons avant de fournir nos coordonnées ou autre renseignements.
- Sur les GAFAM, effacer l'historique après chaque utilisation, consulter le tableau de bord de notre compte pour paramétrer ce qu'on veut qu'il stocke ou partage sur nous.
- Nettoyer ses applications sur smartphones et ordinateurs, c'est-à-dire, bien se déconnecter des comptes quand on supprime une appli et effacer l'historique.
- Attention aux connexions sur les wifi public. Il est recommandé dans ce cas de passer par un VPN.

Propos recueillis par
Vânia Gonçalves