FUTURA

Surveillance : ces appareils du quotidien vous espionnent

Podcast écrit et lu par Emma Hollen

[*Générique d'intro, une musique énergique et vitaminée.*]

Nos appareils connectés nous surveillent-ils ? C'est le décryptage de la semaine, dans Vitamine Tech !

[*Fin du générique.*]

Voici une histoire qui vous est peut-être familière. Vous êtes chez vous, en train de discuter avec un proche autour d'une table. Au détour de votre conversation, vous décidez de lui parler, mettons, au pif, d'un formidable site d'actualité scientifique et technologique que vous avez découvert il n'y a pas longtemps. Intrigué par ce média, qui lui semble ma foi, fort fascinant, votre proche dégaine son portable, bien décidé à voir à quoi il ressemble. Il ouvre le moteur de recherche de Google, et à peine a-t-il tapé un F dans la barre de recherche que le mot Futura lui est suggéré. C'est pourtant la première fois qu'il entend parler de ce site, il ne l'a jamais visité auparavant. Alors, comment Google a-t-il pu deviner ce qu'il allait chercher ? La réponse est assez alarmante, et va même beaucoup plus loin qu'on ne pourrait l'imaginer. Préparez-vous à découvrir que nos smartphones sont loin d'être les seuls à nous espionner.

[*Une musique électronique calme.*]

Le concept d'espionnage téléphonique est probablement aussi vieux… que les téléphones eux-mêmes. Si l'on en croit les sources historiques américaines, il aurait fallu attendre moins de 20 ans après l'avènement de cette nouvelle technologie, ce qui nous mène à peu près dans les années 1890, pour voir la police s'en emparer et mettre les criminels sous surveillance. Avec l'évolution des télécommunications, il fallait donc s'y attendre, les méthodes d'espionnage se sont diversifiées et ont pris de l'ampleur, apportant avec elles leur lot d'inquiétudes. Le sujet revient particulièrement sur le devant de la scène durant des périodes et dans des contextes politiques tendus. Guerres, chasses aux sorcières, dictatures, agitation civile, ou simple climat de méfiance : la crainte d'être mis sur écoute par son gouvernement ou par Interpol revient de manière récurrente – et pas toujours sans raison. Mais depuis quelques temps, il semblerait que ces préoccupations s'étendent de plus en plus souvent… aux entreprises privées. En effet, la police n'aurait plus l'apanage de l'espionnage. Aujourd'hui, il se murmure tout aussi fréquemment que Google, Amazon ou Apple surveillerait nos conversations. Et il faut dire que les scandales provoqués par Alexa, l'assistant vocal d'Amazon, n'ont pas aidé à dissiper les rumeurs. En 2018, plusieurs

conversations auraient été enregistrées par les enceintes connectées de l'entreprise, les Amazon Echo, avant d'être envoyées à des contacts aléatoires des carnets d'adresse de leurs propriétaires. Dès lors, difficile de nier que ces appareils faisaient bien plus que de simplement répondre aux questions avant de s'empresser d'oublier tout ce qu'on venait de leur dire. Petit à petit, Amazon a bien été contraint d'admettre que les commandes et les conversations énoncées par les propriétaires d'Echo pouvaient être enregistrées ou stockées, voire écoutées par des opérateurs humains à travers le monde. Si l'enceinte n'est censée lancer ces enregistrements et leur stockage qu'à partir du moment où le mot « Alexa » est prononcé, les erreurs de compréhension sont toutefois possibles et s'avèrent même fréquentes. Ainsi, selon un rapport de Bloomberg, les employés d'Amazon sont régulièrement exposés à des données sensibles, comme des informations personnelles, des coordonnées bancaires, ou même, dans le cas de deux témoins, des situations de harcèlement sexuel. Les autorités, quant à elles, peuvent émettre un mandat afin d'accéder à ces enregistrements dans le cas d'enquêtes criminelles. Faut-il donc se débarrasser de ces assistants domestiques pour retrouver un peu d'intimité ? C'est un bon début… mais ce n'est pas suffisant !

Si l'on en revient au sujet des smartphones, on peut légitimement se demander si l'assistant virtuel de Google ne tendrait pas l'oreille un peu trop souvent. Bien que l'entreprise ait somme toute réussi à se maintenir hors de cause pour l'instant, ses utilisateurs sont de plus en plus soupçonneux. Par exemple, fréquemment, le moteur de recherche sera un peu trop pertinent dans ses suggestions pour avoir simplement deviné votre requête sur un coup de chance. D'autre fois, Google vous présentera des publicités reprenant des produits que vous auriez pu évoquer lors d'une discussion sans jamais les chercher en ligne. Ces problèmes sont d'autant plus visibles sur les appareils Android, alors, pour les personnes concernées, sachez que vous pouvez modifier les paramètres dans la section Activité sur le Web et dans les applications, afin que le smartphone ne réagisse plus à votre voix. Pour les iPhones, ce sera dans les paramètres de Siri qu'il faudra se rendre. Alors, est-ce qu'on est bon une fois que tout cela est fait ? Toujours pas ! Parce qu'outre les systèmes d'exploitation de vos appareils, les applications que vous y téléchargez sont elles aussi susceptibles d'accéder à votre micro, à votre caméra, ou même à vos fichiers. À chaque fois que vous téléchargez une application, la bonne pratique consisterait à lire de bout en bout ses conditions d'utilisation et à vous assurer de ne lui déverrouiller des portes qu'en cas de nécessité. Par exemple, il est normal d'autoriser une app d'emailing à accéder à vos fichiers si vous avez besoin de joindre un document à votre message ; une app GPS devrait pouvoir accéder à votre localisation ; mais il n'y a en revanche pas de raison pour que l'application SNCF, par exemple, ait besoin d'accéder à votre micro, ce qu'elle ne fait pas d'ailleurs, pour autant qu'on le sache. Et même dans ces cas-là, difficile de contrôler à 100 % qui vous écoute. Récemment, par exemple, l'entreprise américaine Cox Media Group, qui collabore activement avec Facebook, a connu un véritable backlash lorsqu'il a été révélé qu'elle épiait les micros connectés des utilisateurs pour leur délivrer des publicités ciblées avec une précision redoutable. La meilleure option… c'est donc de garder votre smartphone loin de vous tant que vous ne l'utilisez pas, et d'éviter d'avoir des conversations avec ? Ouais… Pas simple !

La même vigilance s'impose d'ailleurs sur un ordinateur. N'autorisez l'accès à vos périphériques d'enregistrement qu'en cas de besoin légitime et sur des sites de confiance, faites attention à ce que vous téléchargez et à ce que vous partagez. Sur internet, pour éviter que votre activité ne soit stockée et analysée, vous pouvez télécharger des bloqueurs de publicité et des trackers, comme l'extension Ghostery ou Privacy Badger.

[*Virgule sonore, une cassette que l'on accélère puis rembobine*.]
[*Une musique de hip-hop expérimental calme*.]

Bon, une fois qu'on a réglé tout ça, on devrait pouvoir être tranquilles. On devrait. Parce que la réalité des appareils connectés… Eh bien, c'est qu'ils sont connectés. Votre smartwatch, votre aspirateur intelligent ou même votre télévision dernière génération peuvent accumuler un certain nombre de données sensibles vous concernant. Cela ne garantit pas que ces informations seront inévitablement dispersées aux quatre vents, mais dans une société où la donnée est la nouvelle monnaie d'échange, il ne faut pas non plus céder à la naïveté. Rien que sur internet, l'UFC-Que Choisir alerte qu'un consommateur qui consulterait à peine 10 sites web serait pisté plus de 4 000 fois par 1 000 entités différentes. Alors, imaginez l'aubaine pour les services commerciaux de pouvoir exploiter les données de l'ensemble de vos appareils pour déterminer avec toujours plus de précision votre profil de consommateur. Dans une étude parue en octobre 2023, un groupe de chercheurs met en évidence la quantité phénoménale d'informations sensibles collectées au sein d'un domicile connecté. Ils révèlent que celles-ci sont compilées sur des serveurs externes et des logiciels tiers, où elles dessinent une carte de vos interactions quotidiennes avec ces objets. Si un seul appareil ne permet pas forcément de dresser un portrait-robot de votre foyer, l'alliance de votre compteur communiquant, de votre smartphone, de votre box et de votre télévision par exemple, peut permettre d'extrapoler une part importante de vos habitudes de vies, des personnes que vous fréquentez, des lieux où vous vous rendez et de vos goûts. Autant dire que ce que l'on appelle la « surveillance commerciale » a encore de beaux jours devant elle.
Et quid alors de la surveillance policière ? Eh bien, celle-ci ne s'arrête pas aux frontières de nos smartphones et de nos recherches internet. Par exemple, si l'on en croit Fanny Guibert, cheffe de rubrique à 60 Millions de Consommateurs et interviewée par France Info, les relevés d'un compteur Linky peuvent être réclamés par la justice pour savoir à quels moments une personne se trouvait chez elle. Plus récemment, la police américaine a établi un nouveau précédent en utilisant pour la première fois le mode sentinelle des Tesla. Si vous ne le savez pas, ces voitures autonomes disposent de caméras haute définition qui servent, bien entendu, à contrôler la route pour savoir où elles vont, mais également à surveiller les parages lorsque le conducteur est absent. Ces caméras s'activent dès que quelqu'un s'approche un peu trop de la voiture, et les vidéos résultantes sont stockées sur une clé USB située dans la boîte à gants. Or, depuis cet été 2024, à San Francisco, les forces de l'ordre ont commencé à demander aux propriétaires d'accéder à ces fameuses clés dans l'élucidation de certaines affaires. Et si le propriétaire de la voiture n'est pas là… qu'à cela ne tienne, on remorque le véhicule !
Ah, et peut-être faudrait-il signaler également que depuis novembre 2023, en vertu de la Loi d'orientation et de programmation du ministère de la justice 2023-2027, les forces de l'ordre françaises ont le droit d'activer à distance les appareils électroniques de suspects pour les localiser, dans le cas de crimes ou de délits punis d'au moins cinq ans de prison. Le texte prévoyait initialement la possibilité de filmer et d'enregistrer les suspects, mais cette mesure a finalement été censurée.
Bref, pour chaque liberté qu'ils apportent, les appareils électroniques nous en retirent au moins autant. Sortirons-nous indemnes de ce pacte faustien ? Les bénéfices dépassent-ils les contraintes ? Dites-nous ce que vous en pensez en commentaire… histoire qu'on en apprenne un peu plus sur vous.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous invite à découvrir notre dernier épisode de Futura FLASH, dans lequel Thibaut Ponamalé vous parle de la mode – peut-être un peu inquiétante et dangereuse – du *mouth taping*. Pour le reste, je vous souhaite une excellente journée ou une très bonne soirée et je vous dis à la prochaine dans Vitamine Tech.

[*Un glitch électronique ferme l'épisode*.]