MUSIQUE — JORJA SMITH, RETOUR AUX SOURCES ÉTATS-UNIS — HUNTER BIDEN, LE BOULET DE SON PÈRE

LIBYE UNE TRAGÉDIE PRÉVISIBLE

Courrier international

N° 1716 du 21 au 27 septembre 2023
courrierinternational.com
France : 4,90 €

Algérie 330 DA, Allemagne 6,30 €, Andorre 6 €, Canada 8,25 $CAN, DOM 6,50 €, Espagne 6,50 €, Grande-Bretagne 5 £, Grèce 6,50 €, Italie 5,50 €, Japon 900 ¥, Maroc 45 DH, Pays-Bas 6 €, Portugal cont. 5,50 €, Sénégal 3400 FCFA, Suisse 7,20 CHF, TOM 1100 XPF, Tunisie 9 DT, Afrique CFA autres 3600 FCFA.

NOS DONNÉES nous trahissent

Un crédit refusé, une offre d'emploi ou une location qui vous échappe? Au-delà du ciblage publicitaire, votre profil numérique affecte directement votre vie. L'enquête à charge du New Scientist.

M 03183 - 1716 - F: 4,90 €

NOS DONNÉES nous trahissent

Pourquoi cette offre d'emploi n'est-elle jamais arrivée jusqu'à vous? Pourquoi n'obtenez-vous pas ce crédit? La faute à vos données personnelles. Au-delà du ciblage publicitaire, elles sont désormais utilisées pour déterminer votre profil psychologique, professionnel ou financier. Il est temps de reprendre le contrôle, affirme *New Scientist*.

—**New Scientist,** *extraits* (*Londres*)

En 2021, un vendredi, je suis entrée dans un hôtel d'Exeter, en Angleterre, à 17 heures, 57 minutes et 35 secondes. Le lendemain matin, j'ai conduit pendant neuf minutes pour me rendre à l'hôpital voisin. J'y suis restée trois jours. Le trajet de retour, qui dure normalement une heure quinze, m'a pris une heure quarante. Pourquoi cette vitesse ralentie? Parce que je transportais mon nouveau-né à l'arrière.

Il ne s'agit pas d'un extrait de mon journal intime. C'est ce que Google sait du jour de la naissance de ma fille, rien qu'avec mon historique de géolocalisation.

Et les données personnelles amassées par d'autres entreprises ce week-end-là leur permettent d'en savoir beaucoup plus encore. Netflix se souvient que j'ai regardé plusieurs comédies légères, dont *Comment se faire larguer en 10 leçons*. Instagram a noté que j'avais liké un post sur l'accouchement déclenché et que je ne me suis pas reconnectée pendant une semaine.

Et alors? Nous savons tous aujourd'hui que la moindre de nos activités en ligne est suivie et que les données collectées sont extrêmement détaillées et s'accumulent en continu. D'ailleurs, peut-être appréciez-vous que Netflix et Instagram connaissent si bien vos goûts.

Pourtant, les enquêtes et procès se multiplient et dressent un tableau où la collecte de nos données a une incidence nettement plus insidieuse que ce que la plupart d'entre nous imaginent. En me penchant sur le sujet, j'ai découvert que la collecte de mes données personnelles pouvait avoir des conséquences sur mes perspectives professionnelles, mes demandes de crédit et mon accès aux soins. Autrement dit, cette pratique a potentiellement des répercussions sur ma vie dont je n'ai même pas idée. *"C'est un immense problème, et chaque jour il y a de quoi être horrifié"*, résume Reuben Binns de l'université d'Oxford.

On pourrait croire qu'avec la mise en place en 2018 du RGPD (Règlement général sur la protection des données) – la loi européenne qui permet aux internautes de mieux contrôler la collecte et l'utilisation de leurs données personnelles –, les questions de vie privée ont été pour l'essentiel résolues. Après tout, il suffit de ne pas accepter les cookies pour ne pas être pisté, non? Alors que je tiens ce raisonnement devant Pam Dixon, représentante du World Privacy Forum, elle part d'un grand éclat de rire incrédule. *"Vous croyez vraiment ça?* me lance-t-elle.

SI VOUS VOUS CROYEZ PROTÉGÉ PAR LES BLOQUEURS DE PUBLICITÉ ET LES VPN, DÉTROMPEZ-VOUS. BON NOMBRE DE CES SERVICES VENDENT AUSSI VOS DONNÉES.

Des centaines d'amendes ont déjà été infligées pour manquement au RGPD, notamment contre Google, British Airways et Amazon. Mais pour les spécialistes, ce n'est que la partie émergée de l'iceberg. Selon une étude menée l'an dernier par David Basin, de l'école polytechnique de Zurich, près de 95 % des sites Internet pourraient être en situation d'infraction.

Alors que la loi devait aider les citoyens à mieux comprendre de quelles données ils autorisent la collecte, plusieurs études montrent que les politiques de confidentialité des marques sont devenues de plus en plus complexes, et non l'inverse. Et si vous vous croyez protégé par les bloqueurs de publicité et les VPN qui masquent votre adresse IP, détrompez-vous. Bon nombre de ces services vendent également vos données.

Nous commençons à peine à mesurer l'ampleur et la complexité du problème. Une poignée d'entreprises – Google, Meta, Amazon et Microsoft – pèsent lourd dans l'équation, reconnaît Isabel Wagner, chercheuse en cybersécurité à l'université de Bâle, en Suisse. Mais derrière eux se cache une myriade d'acteurs qui achètent, vendent, hébergent, pistent et analysent nos données personnelles.

Des centaines de points. Qu'est-ce que cela signifie pour une personne ordinaire comme moi? Pour le savoir, je me suis rendue à Lausanne, à HestiaLabs, une start-up fondée par Paul-Olivier Dehaye, mathématicien et principal lanceur d'alerte dans le scandale de Cambridge Analytica. Ce cabinet de conseil politique avait illégalement utilisé des données d'utilisateurs Facebook pour faire pencher l'élection présidentielle de 2016 en faveur de Donald Trump. L'enquête de Paul-Olivier Dehaye sur Cambridge Analytica a révélé jusqu'où s'étendait le pouvoir d'influence des vendeurs et acheteurs de données. C'est pour changer cela qu'il a créé HestiaLabs.

Avant notre rendez-vous, je demande à plusieurs entreprises de me fournir les données personnelles qu'elles ont enregistrées sur moi – une démarche plus laborieuse qu'on ne serait en droit de le croire depuis le RGPD. Puis, je retrouve Charles Foucault-Dumas, responsable de projet à HestiaLabs, dans les bureaux de la société, un espace de coworking en face de la gare de Lausanne. Installés face à son ordinateur, nous chargeons mes données sur son portail.

Mes données s'affichent devant moi sous la forme d'une carte indiquant tous les endroits où je suis allée, tous les "j'aime" que j'ai distribués et toutes les applications ayant contacté une régie publicitaire. Sur les lieux que je fréquente régulièrement, comme la crèche de ma fille, des centaines de points forment de grosses taches colorées. Mon adresse personnelle est marquée par un énorme point, impossible à manquer. C'est édifiant. Et un peu terrifiant.

SOURCE

NEW SCIENTIST
Londres, Royaume-Uni
Hebdomadaire
newscientist.com
Stimulant, soucieux d'écologie et bon vulgarisateur, *New Scientist* est l'un des meilleurs magazines d'information scientifique du monde. Créé en 1956, il réalise un tiers de ses ventes à l'étranger.

Le plus surprenant est de découvrir quelles applications contactent des services tiers en mon nom. La semaine dernière, le comportement le plus coupable – 29 entreprises contactées – est venu d'un navigateur Internet qui se vante précisément de respecter votre vie privée. Mais, finalement, qu'il s'agisse d'un simple outil de prise de notes ou d'une appli de courses en ligne, à peu près toutes les applications de mon téléphone sollicitent en permanence des entreprises pendant que je vis ma vie.

En règle générale, une entreprise qui vend un produit ou un service s'adresse à une agence de communication faisant le lien avec des plateformes de vente, d'achat et d'échanges d'espaces publicitaires, elles-mêmes connectées à des régies publicitaires chargées de placer les annonces sur un média. Chaque fois que vous allez sur un site Internet ou que vous survolez un message sur un réseau social, toute cette machinerie se met en route – et produit plus de 175 milliards d'euros par an.

SUIS-JE UNE "MAMAN ACCRO À SON PORTABLE", UNE "BONNE VIVANTE", UNE "FACILEMENT DÉCOURAGÉE" OU UNE "WOKE"? JE N'EN SAIS RIEN.

Quelles données personnelles ces entreprises s'échangent-elles? Pour le savoir, il faudrait que je pose la question à chacune d'entre elles. Et même dans le cas de celles que j'ai pu contacter avec l'aide d'HestiaLabs, la réponse n'est pas toujours évidente.

Prenons l'exemple d'Instagram. Le réseau social liste 333 *"centres d'intérêt"* associés à mon profil. Certains sont pour le moins surprenants : le rugby, le festival Burning Man, le marché immobilier et même *"femme à chats"*. Ami lecteur, sache que je n'ai jamais eu de chat.

D'autres sont plus justes, et sans surprise : un certain nombre d'entre eux sont liés à la parentalité, qu'il s'agisse de marques comme Huggies ou Peppa Pig, de discussions sur les lits de bébé ou le sevrage. J'en viens à me demander de quelle manière ces données n'ont pas seulement influencé mes achats mais aussi la vie de ma fille. Sa fascination pour les aventures d'une famille de petits cochons roses est-elle entièrement naturelle ou nous a-t-on *"servi"* ces vidéos en raison de certaines de mes données personnelles transmises par Instagram? Tous ces messages sur le sevrage sont-ils apparus spontanément sur mes réseaux sociaux – influant sur la façon dont j'ai initié ma fille à la nourriture solide – ou ai-je été ciblée? Impossible de reconstruire les liens de cause à effet. J'ignore complètement si mes *"centres d'intérêt"* m'ont désignée pour d'éventuels démarchages.

Les échanges de données personnelles forment un écheveau quasiment impossible à démêler. Il n'est pas rare que des données soient copiées, segmentées et ingurgitées par des algorithmes et des systèmes d'apprentissage automatique. Résultat, explique Pam Dixon, même avec une législation comme le RGPD, nous n'avons pas accès à la totalité de nos données personnelles. *"Il y a un double niveau à ce problème. Il existe une première strate, constituée par les données que nous pouvons retrouver,* poursuit-elle. *Et une seconde que l'on ne voit pas, que nous n'avons légalement pas le droit de voir, personne."*

De récents rapports offrent toutefois quelques aperçus. En juin, une enquête du journal américain *The Markup* a révélé que ce type de données cachées permettait aux publicitaires de nous catégoriser en fonction de nos affinités politiques, de notre état de santé et de notre profil psychologique. Suis-je une *"maman accro à son portable"*, une *"bonne vivante"*, une *"facilement découragée"* ou une *"woke"*? Je n'en sais rien. Ce que je sais, c'est que toutes ces étiquettes sont utilisées par les régies publicitaires en ligne.

Il est perturbant d'apprendre que je suis ainsi étiquetée sans savoir pourquoi ni comment. Une part de moi se demande si c'est vraiment grave. Car je comprends l'intérêt d'avoir des publicités qui tiennent compte de mes préférences, ou d'ouvrir mon application de navigation et de voir apparaître les musées et les restaurants où je suis déjà allée ou qui sont susceptibles de me plaire. Mais, croyez-moi, la désinvolture avec laquelle nous acceptons ce marché est l'un des moyens les plus sûrs de faire grincer des dents un spécialiste de la vie privée.

"Noter" les consommateurs. D'une part, commence Pam Dixon, les utilisations de ces données vont bien au-delà du ciblage publicitaire. Il suffit d'un détail aussi insignifiant que l'enseigne où vous faites vos courses (être client d'une chaîne discount est un indicateur de faible revenu) ou l'achat d'un produit de sport (signe que vous faites de l'exercice) pour modifier votre profil de candidat à l'entrée d'une université ou le montant de votre prime d'assurance médicale. *"On ne parle pas que de publicité ici,* insiste-t-elle. *C'est la vie réelle."*

Aux États-Unis, de récentes lois ont levé le voile sur les pratiques de certaines entreprises. Adopté en 2018 dans le Vermont, le Data Broker Act a ainsi révélé que les courtiers en données enregistrés dans cet État – mais également présents dans d'autres – vendaient des données personnelles à de potentiels employeurs ou bailleurs, souvent via des intermédiaires. En juillet, le bureau américain de protection financière du consommateur a découvert que des données cachées servaient à "noter" les consommateurs, un peu de la même manière que les banques vous attribuent une note financière globale lorsque vous faites une demande de prêt. Reuben Binns explique : *"Il y a les choses que vous faites, les sites que vous visitez, les applications que vous utilisez, tous ces services peuvent alimenter des plateformes qui vérifient si vous êtes un bon candidat à la location et quelles conditions de crédit vous proposer."*

À HestiaLabs, je comprends que j'ai peut-être moi aussi été affectée par ces pratiques dans mon quotidien, pas seulement à travers le ciblage publicitaire mais également par la façon dont mes données sont traitées par les algorithmes.

Repères

QU'EST-CE QUE LE RGPD?

Le règlement général sur la protection des données (RGPD) s'applique depuis le 25 mai 2018 dans l'ensemble des 27 pays de l'Union européenne. Ce texte vise essentiellement à renforcer le droit des personnes concernées par le traitement de leurs données à caractère personnel.
On entend par là toute information se rapportant à une personne physique : nom, prénom mais aussi numéro de client, de téléphone, de sécurité sociale ou encore magasin dans lequel elle fait ses achats, centres d'intérêt… et la liste est longue.
L'une des dispositions du RGPD est le consentement "explicite" et "positif". Par exemple, sur Internet (sites web, applications, réseaux sociaux, etc.), un citoyen doit pouvoir choisir s'il accepte ou non les cookies – en clair, s'il accepte que de petites quantités de données soient stockées et échangées avec un serveur.

En effet, sur LinkedIn, un des présupposés liés à mon profil indique que je ne suis ni *"une personnalité de leader"* ni *"un manager senior"*. Alors que j'ai dirigé une équipe de 20 personnes à la BBC et qu'avant cela j'ai été rédactrice en chef de plusieurs sites web de la chaîne – autant d'informations que j'ai spécifiquement compilées sur mon profil LinkedIn. Cela a-t-il une incidence sur mon évolution professionnelle? Lorsque je pose la question à un représentant de la plateforme, on m'assure que ces *"présupposés"* ne sont aucunement utilisés *"pour sélectionner les offres d'emploi qui* [me] *sont proposées sur ce réseau"*.

Pourtant, plusieurs actions en justice ont révélé que, sur Facebook, des données étaient utilisées afin de cacher aux femmes certaines offres d'emploi dans le secteur des technologies. En 2019, la maison mère du réseau, Meta, a supprimé cette possibilité pour les annonceurs. Sauf qu'il est très facile de trouver d'autres moyens d'exclure les femmes, soulignent les spécialistes,

"ON NE PARLE PAS QUE DE PUBLICITÉ ICI. C'EST LA VIE RÉELLE."

Pam Dixon, REPRÉSENTANTE DU WORLD PRIVACY FORUM

← *Sur les mains : Privé. Dessin de* **Peter Arkle** *paru dans* **Business Week,** *New York.*

par exemple en ciblant les profils comportant des intérêts associés à des stéréotypes masculins. *"Ces préjudices ne sont pas visibles sur le moment pour l'utilisateur. Ils sont souvent très abstraits et peuvent intervenir très tard dans le processus de filtrage"*, explique Isabel Wagner.

Manque de transparence. Plus le volume de données collectées augmente, plus la liste des problèmes signalés dans les médias s'allonge. Des applications de suivi d'ovulation – ainsi que des SMS, des courriels et des recherches sur Internet – ont été utilisées pour lancer des poursuites contre des femmes s'étant fait avorter aux États-Unis depuis la suppression de l'arrêt Roe *vs* Wade [qui a provoqué en juin 2022 un retour à la situation d'avant 1973, quand chaque État était libre d'interdire ou non l'avortement].

Des prêtres ont vu leur homosexualité dévoilée après qu'ils ont utilisé l'application de rencontre Grindr. Un officier russe a été tué lors de son jogging matinal après avoir été suivi, présume-t-on, par l'intermédiaire des données publiques de son compte Strava. La protection des données vise à empêcher ce genre de problèmes. *"Mais de toute évidence la mise en œuvre laisse fortement à désirer"*, soupire Reuben Binns.

Le problème tient en partie au manque de transparence des entreprises. Nombre d'entre elles optent pour des systèmes *"protégeant la vie privée"* où les données d'une personne sont segmentées en plusieurs points de données qui sont disséminés dans différents serveurs ou localement chiffrés. Paradoxalement, cela complique surtout la tâche pour l'utilisateur qui souhaite accéder à ses propres données et comprendre comment elles sont utilisées.

Du point de vue de Paul-Olivier Dehaye, d'HestiaLabs, il ne fait aucun doute que les entreprises peuvent et doivent nous rendre le pouvoir sur nos données. *"Si vous allez sur un site maintenant, une multitude d'entités en seront informées dans la seconde et sauront qui vous êtes et sur quel site vous avez commandé une paire de baskets il y a deux semaines. Dès lors que l'objectif est de vous inonder de mauvaises pubs, les entreprises sont capables de résoudre tous les problèmes. Mais demandez-leur vos données, et elles ne savent plus rien faire. Mais il existe un moyen de mettre cette force du capitalisme à votre service plutôt qu'au leur."*

J'espère qu'il a raison. Alors que je marche dans les rues de Lausanne après avoir quitté les bureaux d'HestiaLabs, je vois un homme devant la vitrine d'un magasin de couteaux, son téléphone portable dépassant de sa poche, puis une femme tirée à quatre épingles, un sac Zara dans une main et son portable dans l'autre. Un peu plus loin, un homme parle avec animation dans son téléphone devant le commissariat de police.

"SI VOUS ALLEZ SUR UN SITE MAINTENANT, UNE MULTITUDE D'ENTITÉS EN SERONT INFORMÉES DANS LA SECONDE ET SAURONT QUI VOUS ÊTES."

Paul-Olivier Dehaye, LANCEUR D'ALERTE DU SCANDALE CAMBRIDGE ANALYTICA

Pour eux comme pour moi, tous ces instants sont aussi brefs qu'insignifiants. Mais pour les entreprises qui collectent nos données, ce sont autant d'occasions à saisir. Des opportunités monnayables. Et tous ces points de données ne disparaîtront peut-être jamais.

Suivant les conseils de Paul-Olivier Dehaye et des autres spécialistes que j'ai interrogés, je décide en rentrant chez moi de faire le tri dans mon téléphone et de supprimer les applications dont je ne me sers pas. Je me débarrasse également de celles que j'utilise peu et qui contactent un peu trop d'entreprises ; je les utiliserai depuis mon ordinateur portable à la place. (J'utilise un service appelé "TC Slim" qui m'indique quelles entreprises sont en lien avec mes applications.) J'installe également un nouveau navigateur qui respecte réellement – semble-t-il – ma vie privée. Les applications open source et non commerciales sont généralement de bonnes solutions, explique Isabel Wagner, car leurs développeurs ont moins d'intérêt à collecter vos données.

J'ai également commencé à éteindre mon téléphone lorsque je ne m'en sers pas. Car la plupart des téléphones continuent à transmettre vos données de géolocalisation même lorsque vous coupez la connexion wifi ou activez le mode avion. Sur mon compte Google, j'ai décoché l'option de sauvegarde des lieux.

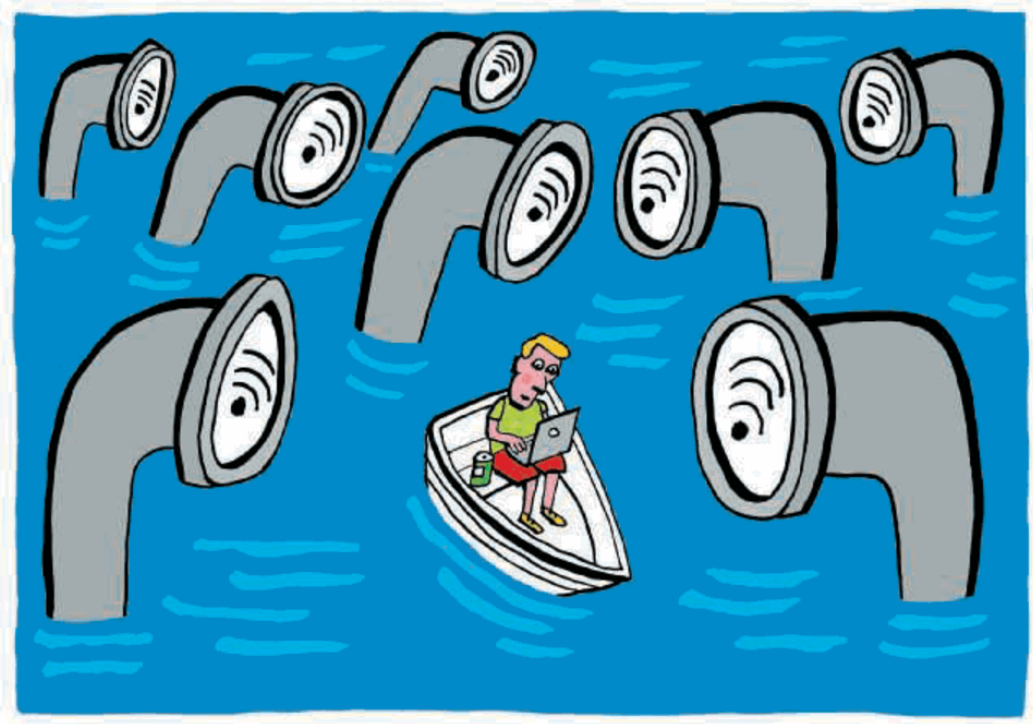
On peut également modifier notre façon de payer. Pam Dixon préconise d'avoir plusieurs cartes bancaires et de choisir *"minutieusement"* lesquelles utiliser sur Internet. Pour les achats susceptibles d'envoyer un signal *"négatif"*, dans un magasin discount par exemple, préférez les paiements en liquide. Elle recommande également d'éviter les sites et applications liés à la santé. *"C'est un terrain miné en général"*, résume-t-elle.

"C'est un jeu où on ne peut que perdre", conclut Paul-Olivier Dehaye. Raison pour laquelle la solution ne relève pas des seuls individus. *"Nous avons besoin d'un véritable changement sociétal"*, confirme Reuben Binns. Si suffisamment de gens parviennent à faire entendre leur voix, nous pourrons faire évoluer le système, espère Paul-Olivier Dehaye. La première étape consiste à faire une demande d'accès à vos données personnelles. *"Faites comprendre aux entreprises que si elles font un pas de travers vous ne leur ferez plus confiance,* résume-t-il. *À l'ère des données, si vous perdez la confiance des gens, votre entreprise est condamnée."*

—Amanda Ruggeri,
publié le 23 août

La Californie montre l'exemple

●●● Une victoire pour le respect de la vie privée vient d'être remportée en Californie : les citoyens de cet État américain auront la possibilité d'effacer facilement leur empreinte numérique à partir de 2026. *"Les législateurs californiens ont adopté [le 12 septembre] un projet de loi qui devrait permettre aux consommateurs de contraindre les courtiers en données à supprimer toutes les informations les concernant, sur simple et unique demande"*, rapporte le **Los Angeles Times.** Un gain de temps non négligeable quand on sait qu'environ 500 courtiers en données sont enregistrés en Californie, et que la plupart d'entre eux n'ont jamais été en contact direct avec le consommateur, mais qu'ils disposent de certaines informations grâce à l'achat de bases de données par exemple. Pour le moment, et malgré la loi californienne sur la protection de la vie privée adoptée en 2018, il est difficile de savoir de quelles informations les entreprises disposent. Elles peuvent refuser d'effacer les données des personnes qui le leur demandent ou tout simplement ne pas répondre. Ce qui ne sera plus autorisé en 2026.



↑ *Dessin de* **Schot,** *Pays-Bas.*

Mon clavier est un espion

Indispensables en Chine, les applications destinées à faciliter la saisie des caractères ne sont pas sans risque. Des chercheurs viennent de révéler une grave faille de sécurité dans l'une des plus utilisées.

—MIT Technology Review, *extraits (Cambridge, États-Unis)*

Le premier logiciel que téléchargent des millions de Chinois sur un nouvel ordinateur portable ou un nouveau smartphone est toujours le même : une application de clavier. Mais rares sont ceux qui ont conscience qu'ils [permettent ainsi] à des yeux espions de consulter tout ce qu'ils tapent.

Comme des dizaines de caractères chinois se transcrivent phonétiquement de la même manière en alphabet latin, un clavier de type QWERTY classique n'est pas pratique du tout. Une application de clavier bien conçue peut faire gagner beaucoup de temps, car elle prédit les caractères et les mots que l'utilisateur veut saisir. Aujourd'hui, plus de 800 millions de Chinois utilisent ce genre d'applications tierces sur leurs PC et téléphones mobiles.

Mais un récent rapport du Citizen Lab, un groupe de recherche sous la tutelle de l'université de Toronto, spécialisé dans les technologies et la sécurité, révèle que Sogou Input Method, l'une des applis de clavier chinois les plus populaires, présentait une énorme faille de sécurité.

"C'est une application qui manie des informations très sensibles, puisqu'elle sait tout ce qu'on tape", explique Jeffrey Knockel, chercheur associé senior au Citizen Lab et coauteur du rapport. Avec ses collègues, il a découvert que le système de cryptage de Sogou pouvait être exploité pour intercepter et décrypter avec précision ce qu'on saisissait, en temps réel.

Sogou, qui a été racheté par le géant des hautes technologies Tencent en 2021, a rapidement corrigé cette faille après que les chercheurs du Citizen Lab l'ont révélée à l'entreprise.

"Accès complet" à l'appareil. Mais rien ne garantit qu'elle soit la seule de l'application, et les chercheurs ne se sont pas penchés sur d'autres applications de clavier très appréciées sur le marché chinois. Autrement dit, ce genre de logiciels très répandus va continuer de représenter un risque de sécurité pour des centaines de millions de personnes. Ce qui est particulièrement inquiétant, c'est que certaines communications censées être cryptées – grâce à des applications comme Signal, par exemple – deviennent ainsi exposées aux systèmes de surveillance de l'État chinois.

Les applications de clavier, également connues sous le nom d'IME [sigle anglais pour *input method editor*, éditeur de méthode d'entrée], sont nécessaires pour entrer du texte dans des langues dont le nombre de caractères est supérieur à ce qu'un clavier courant en alphabet latin peut contenir. C'est le cas avec les caractères japonais, coréens ou indiens notamment. De leur côté, les utilisateurs chinois sont quasiment obligés d'avoir un IME.

"Lorsque l'on saisit des caractères chinois à partir d'un alphabet latin, on se trouve confronté à de nombreuses ambiguïtés", explique Mona Wang, membre de l'Open Technology Fund au Citizen Lab et coautrice du rapport. Une même transcription phonétique peut correspondre à des dizaines, voire à des centaines de caractères chinois, lesquels peuvent par ailleurs être associés de différentes manières pour former des mots. Une application de clavier adaptée à la langue chinoise se montre donc beaucoup plus performante que le clavier d'origine.

Depuis l'arrivée des ordinateurs personnels, les développeurs chinois ont proposé toutes sortes d'IME pour accélérer la frappe, certains abandonnant même le système de transcription phonétique au profit du dessin sur écran ou du choix de parties d'idéogrammes. Par conséquent, tout le monde a pris l'habitude en Chine de télécharger un logiciel de clavier alternatif.

L'an dernier, Baidu Input Method arrivait en tête des applications de clavier en Chine, avec 607 millions d'utilisateurs et 46,4 % de part de marché, contre encore 561 millions d'utilisateurs pour Sogou Input Method, selon iiMedia Research, un cabinet d'analyse chinois.

Une application de clavier peut accéder à de très nombreuses informations sur son utilisateur. Ainsi, lorsqu'on télécharge et ajoute aux options du clavier d'un iPhone l'application Sogou, celle-ci demande un *"accès complet"* à l'appareil. Si l'utilisateur donne son accord, tout ce qu'il tapera sera susceptible d'être envoyé sur un serveur Sogou dans le cloud.

C'est cette connexion au cloud qui est le secret de la réussite de la plupart des IME. Elle leur permet d'améliorer la suggestion de texte et de proposer d'autres fonctions, comme la recherche de GIF et de mèmes. Le revers de la médaille est que cela accroît les risques puisque du contenu peut être intercepté pendant sa transmission.

PLUS DE 800 MILLIONS DE CHINOIS UTILISENT CE GENRE D'APPLICATIONS TIERCES SUR LEURS PC ET TÉLÉPHONES.

Il est de la responsabilité des applications de chiffrer les données pour empêcher que cela ne se produise. Selon la charte de Sogou, l'entreprise a *"pris toutes les mesures technologiques de sécurité standard nécessaires* [...]*"* pour éviter au maximum un *"accès non autorisé"* aux informations personnelles des utilisateurs, ainsi que toute *"fuite, destruction, utilisation abusive, divulgation non autorisée ou altération"* de celles-ci.

Mona Wang le rappelle : *"Les gens se méfient généralement [des applications de clavier] parce qu'elles font de la publicité pour leur service dans le cloud. Il ne fait quasiment aucun doute qu'elles diffusent sur Internet un certain nombre de données sur les frappes de texte."*

Malgré cela, les utilisateurs continuent de leur accorder un accès total à leur appareil.

Mais tous les mots ne sont pas transmis dans le cloud, selon les constatations des chercheurs. *"Quand on tape quelque chose comme* nihao [*'bonjour', en chinois*], [*l'application*] *peut réagir sans avoir à utiliser la base de données sur le cloud, mais elle doit y faire appel quand on veut entrer quelque chose de plus compliqué et, disons-le, plus intéressant…"* explique Jeffrey Knockel.

En plus du contenu saisi, Jeffrey Knockel et ses collègues du Citizen Lab ont obtenu d'autres informations comme les identifiants techniques de l'appareil de l'utilisateur, des renseignements sur l'application qui a permis la frappe, et même une liste des applications installées sur l'appareil.

Arrestation d'étudiants. De nombreuses personnes malintentionnées, comme des cybercriminels à la recherche d'informations privées (adresses postales, numéros de compte bancaire) ou des pirates informatiques travaillant pour les pouvoirs publics, souhaiteraient sans doute exploiter ce genre de faille pour se livrer à de l'espionnage, font observer les chercheurs.

En l'occurrence, la faille a été comblée par une mise à jour du logiciel Sogou Input Method par Tencent sur toutes ses plateformes fin juillet.

Partout dans le monde, ceux qui sont dans le collimateur des autorités se tournent vers des applications proposant un chiffrement de bout en bout. Mais avec la vulnérabilité des applications de clavier, des applications de communication chiffrée comme Signal ou WhatsApp deviennent également peu sûres. En outre, lorsqu'un IME est piraté, même une application qui n'est pas en ligne, comme l'application par défaut d'un ordinateur portable, peut également présenter un risque en matière de sécurité.

Dès 2019, Naomi Wu, qui habite Shenzhen et tient un blog sur les hautes technologies sous le pseudo de SexyCyborg, alertait déjà sur les risques liés à l'utilisation d'applications de clavier chinoises avec Signal. Elle soupçonnait même cette messagerie d'avoir conduit à l'arrestation par la police, en 2018, d'étudiants militants chinois qui l'utilisaient pour communiquer avec des journalistes étrangers.

En janvier 2021, Signal a tenu à clarifier la situation, affirmant que sa fonction "clavier incognito" (qui ne fonctionne que pour les utilisateurs de systèmes Android, plus vulnérables que les iOS) n'était pas un outil de confidentialité infaillible. *"Les claviers et IME sur Android peuvent ignorer le mode 'clavier incognito'. Cette option d'Android n'est qu'une solution préventive et ne constitue pas une garantie. Il est important d'utiliser un clavier ou un IME dans lequel vous avez confiance. Signal ne peut ni détecter ni protéger votre appareil des logiciels malveillants"*, a ajouté l'entreprise sur sa page web consacrée à la sécurité des claviers.

Les récentes conclusions du Citizen Lab viennent étayer les soupçons de Naomi Wu. Le risque est particulièrement élevé pour les utilisateurs chinois, plus susceptibles d'utiliser des applications de clavier et qui font l'objet d'une surveillance sévère de la part de leur gouvernement. (Naomi Wu a elle-même disparu des réseaux sociaux depuis la fin du mois de juin, à la suite d'une descente de police à son domicile, consécutive sans doute à ses propos en ligne sur Signal et les applications de clavier).

Mais d'autres gouvernements accordent également beaucoup d'attention au problème de vulnérabilité dans la transmission de données cryptées. Ainsi, dans un document de 2012 divulgué par Edward Snowden, on apprend que l'alliance des services de renseignements Five Eyes (qui comprend le Canada, les États-Unis, la Grande-Bretagne, l'Australie et la Nouvelle-Zélande) a discrètement exploité une faille similaire du navigateur UC Browser, très populaire en Chine, pour intercepter certaines transmissions.

Les informations de frappe obtenues par le biais d'applications de clavier ne sont pas seulement très convoitées par les agents de l'État, elles peuvent aussi être vendues, divulguées et piratées à d'autres fins. En 2021, après avoir eu accès à des données personnelles grâce aux IME de Sogou, Baidu et autres applications du même genre, des annonceurs les auraient utilisées pour diffuser des publicités personnalisées.

AVEC LA VULNÉRABILITÉ DES APPLICATIONS DE CLAVIER, DES APPLICATIONS CHIFFRÉES COMME SIGNAL DEVIENNENT ÉGALEMENT PEU SÛRES.

Ces problèmes de sécurité ne sont pas propres aux applications chinoises. En 2016, les utilisateurs de SwiftKey, un IME racheté par Microsoft cette année-là, ont eu la surprise de constater que l'application remplissait automatiquement les adresses électroniques et les informations personnelles d'autres personnes; c'était la conséquence d'un bogue dans le système de synchronisation dans le cloud. L'année suivante, une application de clavier virtuel a divulgué par mégarde les données personnelles de 31 millions d'utilisateurs.

Même si la faille identifiée par Citizen Lab chez Sogou a été corrigée rapidement, on peut s'attendre à la révélation sous peu d'une autre faille de sécurité dans une application de clavier, compte tenu de toutes ces brèches.

Comme le fait remarquer Jeffrey Knockel, l'utilisation de Sogou et d'autres applications similaires présente toujours des risques de sécurité, en particulier en Chine, où toutes les applications ont l'obligation légale de fournir des données au gouvernement s'il le leur demande. *"Si cela vous gêne,* remarque le chercheur, *vous pouvez tout simplement vous interroger sur la nécessité d'utiliser Sogou Input Method. Point barre."*

—Zeyi Yang,
publié le 21 août

À lire

Comment les Chinois perçoivent-ils la censure et le contrôle numérique que leur impose un pouvoir de plus en plus autoritaire? Dans une enquête intitulée *La Société de surveillance made in China*, parue aux éditions de l'Aube en février, **Zhang Zhulin,** journaliste à *Courrier international*, livre des témoignages glaçants sur la vie quotidienne sous le régime de Xi Jinping.

Des voitures très indiscrètes

●●● Ne vous fiez pas à votre voiture. C'est la conclusion qu'on peut tirer de la dernière enquête de la Fondation Mozilla. Cette association à but non lucratif évalue régulièrement le respect de la vie privée des utilisateurs qu'offrent les objets connectés et les applications en ligne. *"Toutes les marques de voiture que nous avons examinées [25 au total] récoltent beaucoup plus de données personnelles que nécessaire et utilisent ces informations à de tout autres fins que de simplement faire fonctionner votre véhicule et répondre à vos besoins"*, fait savoir **Mozilla.** Pire, certaines grandes marques comme Cadillac, Chevrolet et d'autres indiquent dans leur déclaration de confidentialité qu'elles peuvent enregistrer des données sur les *"caractéristiques génétiques, physiologiques, comportementales et biologiques"* des personnes. En outre, plus de 84 % des marques vendent ou partagent les données récoltées. Seules deux marques, Renault et Dacia (qui appartiennent au même groupe automobile), assurent à leurs conducteurs le droit d'effacer leurs données. *"Ce n'est pas un hasard si les voitures qui collectent le moins de données sont seulement disponibles en Europe, qui est protégée par le très sérieux règlement général sur la protection des données (RGPD)"*, notent les auteurs.

SOURCE

MIT TECHNOLOGY REVIEW
Cambridge, États-Unis
Bimestriel
techreview.com
Fondée en 1899, la revue est installée sur le campus du célèbre Massachusetts Institute of Technology (MIT) et s'adresse aux ingénieurs, scientifiques et hommes d'affaires soucieux de s'informer des nouvelles tendances technologiques et des décisions politiques en la matière. Le magazine papier est consultable gratuitement sur le site, qui propose également une production exclusive.