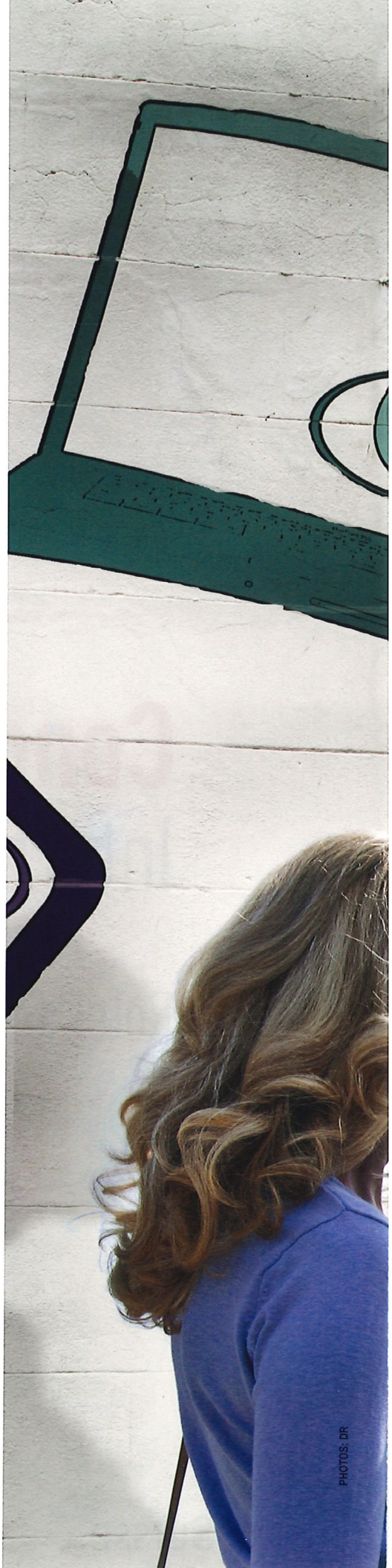
SMARTPHONE: PEUT-ON ÉCHAPPER À CET ESPION?



LA TOILE D'INTERNET EST DEVENUE UN FILET POUR COLLECTER NOS DONNÉES PERSONNELLES AFIN DE PROFILER NOS GOÛTS DE CONSOMMATEURS MAIS AUSSI NOS OPINIONS D'ÉLECTEURS. JUSQU'OÙ CETTE INTRUSION PEUT-ELLE ALLER? EXISTE-T-IL DES OUTILS QUI PROTÈGENT NOTRE INTIMITÉ?

PAR FABRICE DELAYE

PHOTOS: DR

COMMENT NOS SMARTPHONES NOUS ESPIONNENT

OLGA LUKYANOVA et André Mintz sont deux artistes digitaux. En 2016, ils ont lancé le projet deadartist.me, un petit jeu apparemment futile sur Facebook. Il consistait à découvrir de quel artiste on est la réincarnation. Grâce à l'accès au profil des participants et à celui de leurs amis qu'acceptaient les utilisateurs cliquant sur les conditions générales de deadartist.me, le tandem a reconstitué des milliers de cartes de diffusion de nouvelles, de réseaux d'amis... Quelque chose d'assez graphique. Olga Lukyanova et André Mintz n'imaginaient pas que leur projet annonçait le plus grand scandale de l'histoire des réseaux sociaux: l'affaire Cambridge Analytica.

Ce dont Cambridge Analytica est le nom

Ce scandale qui éclate en mars dernier contient en lui-même toutes les dérives rendues possibles avec la moisson systématique d'informations personnelles et leur traitement par des technologies de big data et de plus en intelligence artificielle utilisées par les géants d'internet. Après les révélations du lanceur d'alerte Edward Snowden, le monde avait pris conscience des moyens démesurés déployés par les Etats pour la surveillance électronique. «Avec Cambridge Analytica, on réalise que les technologies utilisées pour le ciblage publicitaire peuvent servir à la propagande politique et à la manipulation des opinions», explique Alexis Fitzjean O'Cobhthaigh, avocat et membre de la Quadrature du net, principale ONG qui milite en France contre la surveillance électronique.

Il faut dire que l'affaire Cambridge Analytica, c'est un peu un épisode de la série *Black Mirror*. En l'espèce, l'entreprise britannique a mis en place un questionnaire d'apparence anodine (sous couvert de recherche universitaire) qu'elle a diffusé sur Facebook. Cela lui a permis de récupérer les données personnelles des 270 000 utilisateurs qui ont répondu au questionnaire et à travers l'outil Social graph de leurs amis Facebook. Au total, les données de 87 millions d'utilisateurs, leurs like, leurs photos... situés pour l'essentiel aux Etats-Unis.

Cela ne s'arrête pas là. Cambridge Analytica a ensuite croisé ces informations avec les données qu'on peut acheter chez les data brokers américains (notes de crédit utilisées par les banques, marques de voitures achetées...). Puis, elle a mouliné ces informations au travers de son modèle de profilage psychologique. Selon les déclarations au *Guardian* de Christopher Wylie, employé de Cambridge Analytica qui a lancé l'alerte: «Nous nous sommes servis de Facebook pour récupérer le profil de millions de personnes. Nous avons construit des modèles pour exploiter ces connaissances et cibler leurs démons intérieurs.»

Il est de notoriété publique que ces informations ont servi lors de la campagne de Donald Trump. Sans conséquence pour le président américain. Même si Facebook a coupé les ponts avec Cambridge Analytica à la veille du scandale, que son CEO, Mark Zuckerberg, a dû s'expliquer en avril devant le Congrès américain, et qu'elle vient d'être condamnée par la justice britannique à une amende de 500 000 livres (le maximum en fonction de la loi en vigueur à l'époque des faits) pour «infractions sérieuses à la loi sur la protection des données», au final, l'entreprise a bien apporté quelques correctifs mais sa manière d'opérer n'a pas changé fondamentalement.

Lanceurs d'alerte

Comment le pourrait-elle? Comme l'explique la sociologue Zeynep Tufekci dans le documentaire en deux volets que *Frontline*, l'émission phare du journalisme d'investigation aux Etats-Unis, vient de diffuser sur Facebook: «Le modèle d'affaires de Facebook est basé sur une machine de surveillance.» On apprend ainsi comment l'entreprise constitue des «shadow profiles» de gens qui ne sont même pas utilisateurs du réseau. Et comment elle utilise des micro-images cachées dans un contenu afin de suivre dans le détail la navigation des internautes (c'est une des technologies à la base du ciblage publicitaire qui fait qu'une pub vous suit comme par magie de site en site).

«On réalise que les technologies utilisées pour le ciblage publicitaire peuvent servir à la propagande politique et à la manipulation des opinions» Fitzjean O'Cobhthaigh, avocat

Christopher Wylie, employé de Cambridge Analytica, a alerté l'opinion sur l'utilisation des profils.

Cependant, si Facebook a été placé en première ligne par l'affaire Cambridge Analytica, c'est en réalité toute l'économie numérique qui est confrontée au même dilemme. «Le modèle actuel oblige les utilisateurs à fournir leurs données aux géants du web en échange d'un service. Et, comme nous l'avons tous découvert, cela n'a pas été dans notre meilleur intérêt», analyse sur son blog, en septembre dernier, Tim Berners-Lee, coinventeur du World Wide Web lorsqu'il était au CERN à Genève.

Il n'est pas le seul «insider» à s'inquiéter. Le directeur juridique de Microsoft, Brad Smith, appelait récemment les gouvernements à encadrer l'usage de la reconnaissance faciale. D'anciens cadres de Facebook comme Chamath Palihapitiya (ex-vice-président pour la croissance des utilisateurs) ou de Google, comme Guillaume Chaslot (ex-ingénieur de YouTube), sont devenus des lanceurs d'alerte.

Lors de sa présentation devant le Parlement européen à Bruxelles le 24 octobre dernier, le patron d'Apple, Tim Cook, a été jusqu'à déclarer que «le rassemblement des informations numériques par les entreprises s'était transformé en une arme agissant contre les particuliers avec une efficacité militaire». Il a ajouté que «les algorithmes qui nous facilitent la vie savent également parfaitement faire ressortir nos pires défauts» avant d'appeler à une version américaine du Règlement général sur la protection des données (RGPD) entré en vigueur dans l'Union européenne en mai dernier.

Forcément, entendre le patron d'un des GAFAM (Google, Apple, Facebook, Amazon, Microsoft) s'émouvoir de cette surveillance généralisée interroge. Certes, Apple s'est fait le champion de la protection des données. Cela étant, comme le remarque Bernard Benoit, responsable de White Noise, le système de cryptage pour la téléphonie mobile du groupe Kudelski, «l'administration américaine utilise principalement des téléphones Samsung coréens pour les communications sécurisées».

Bonne question qui renvoie à celle de savoir comment nos informations personnelles sont collectées? En bref: avec, mais aussi sans notre consentement et dans la plus grande opacité.

L'écosystème de la surveillance

Le premier niveau de cette collecte géante, c'est celui des applications. «Beaucoup collectent davantage de données que ce qu'elles annoncent», relève Bernard Benoit. Y compris la plupart de celles qui n'ont à première vue rien à voir avec Facebook, Amazon et consorts. «Pour aller vite, les développeurs d'applications ont recours à des librairies tierces ou API», explique Julien Probst, vice-président chargé des initiatives stratégiques de l'entreprise de cybersécurité InfoSec Global. C'est ce qui permet d'ajouter des fonctionnalités comme le login simplifié à partir de son compte Facebook ou LinkedIn, d'ouvrir Google Maps pour la géolocalisation ou qu'une application demande l'accès au carnet d'adresses, à la caméra, au micro...

Pour répondre à des besoins de statistiques, ces API propriétaires renvoient systématiquement de l'information à leurs éditeurs d'origine. Ne serait-ce que pour compter le nombre d'utilisateurs et répertorier les dispositifs mobiles. «Mais on ne sait pas toujours ce qui est partagé comme information», poursuit Julien Probst. «Le code de ces API propriétaires n'étant pas ouvert, on ne sait pas ce qui se passe», résume Alexis Fitzjean O'Cobhthaigh.

Grâce à des travaux de recherche, on en a quand même une petite idée. Des chercheurs de l'Université Northeastern à Boston ont, par exemple, voulu vérifier

VOUS AUSSI, ESPIONNEZ VOS AMIS

«La seule application d'espionnage Android qui capture toutes les formes de messagerie. Espionnez n'importe quel ordinateur avec notre puissant logiciel de surveillance informatique.» Le moins que l'on puisse dire, c'est que les messages publicitaires du site de Flexispy n'y vont pas par quatre chemins. Comme d'autres logiciels espions (MSpy, Life 360... Une étude en a dénombré 300), cette application est en vente libre sous prétexte d'un usage officiel destiné à surveiller ses enfants ou ses employés. Ce qui n'empêche pas de la détourner. Car une fois installée, Flexispy est non seulement cachée à l'utilisateur mais elle peut lire toutes les messageries, enregistrer la saisie sur clavier et même ouvrir le microphone à distance. Certes, il faut installer ces spywares. Et payer ensuite un abonnement de près de 70 francs par mois dans le cas de Flexispy. Mais si c'est facile pour une PME de vendre de tels produits, on n'ose imaginer ce que peuvent faire des acteurs équipés de moyens beaucoup plus importants.

PHOTO: REUTERS

Karl Aberer, professeur à l'EPFL: «Tout est potentiellement collecté.»

Florent Schlaeppi, CEO de Business-Monitor.ch, insiste sur le rôle des outils d'analyse.

si, comme le prétend une légende urbaine, certaines apps écoutent nos conversations au travers du micro de notre smartphone. Pour ce faire, ils ont testé 17 260 des applications les plus populaires sur Android, y inclus Facebook et 8000 autres apps qui renvoient des informations au réseau social.

Résultat? Pas la moindre trace d'ouverture intempestive des micros. Par contre, un détail troublant: nombre de ces apps font des photos ou des vidéos pour capturer l'écran de l'utilisateur qu'elles envoient à des tiers comme Appsee, entreprise d'analyses des données mobiles. Sans que rien ne l'indique nulle part...

Dans un registre comparable, le professeur Karl Aberer et son équipe du laboratoire des systèmes d'information distribuée à l'EPFL ont fait une curieuse découverte dans les applications de Drive, service cloud de Google. «Environ deux tiers de la centaine d'apps (construites par des tiers pour exploiter ce service) que nous avons analysées bénéficient d'accès surprivilégiés», explique-t-il. En d'autres termes, elles ont accès à des informations dont elles n'ont pas besoin pour remplir leurs fonctions. Il cite l'exemple d'un convertisseur PDF qui a accès à la bibliothèque musicale ou à l'album photos géolocalisées de l'utilisateur... «Pourquoi, si ce n'est pour moissonner des données personnelles?»

Tout est collecté

Certes, dans ces deux cas, ce sont des développeurs tiers qui utilisent les plateformes des géants du net pour obtenir plus d'informations personnelles. Mais personne n'a vraiment de doute sur le fait que ces derniers collectent plus d'informations sur nous que ce que nous leur donnons déjà en toute conscience. «Tout est potentiellement collecté», affirme simplement Karl Aberer.

Des chercheurs de l'Université de Vanderbilt, à Nashville, ont ainsi rendu publique une étude en août dernier sur la manière dont Google collecte des informations activement (via l'utilisation de ses produits comme Chrome ou YouTube), mais aussi passivement. Ils ont montré qu'un téléphone Android – même inactif et immobile – se connecte 900 fois par jour avec les serveurs de Google, dont pas moins de 300 fois pour communiquer sa position.

CEO de la plateforme d'informations économiques Business-Monitor.ch, Florent Schlaeppi ajoute à ce tableau le rôle des outils d'analytique. «Beaucoup de webmasters utilisent Google Analytics qui, par construction, partage les données avec Google. Vous pouvez être un développeur suisse, hébergé en Suisse, si vous utilisez cet outil, fatalement vous allez partager les informations sur le trafic de votre site avec Google. C'est une des raisons pour lesquelles les grandes entreprises qui veulent garder ces informations utilisent des outils d'analyse payants.» Chez Kudelski, Bernard Benoit pointe le cas similaire du push notification pour applications mobiles Firebase de Google. «Il collecte l'âge, le sexe, le pays de résidence, les intérêts de la personne, sa langue, y compris si l'application tourne sur iOS d'Apple.»

Les utilisateurs se méfient

Certes, cette collecte frénétique de données est légale. Elle est généralement justifiée par l'idée de fournir une meilleure expérience utilisateur. Mais, en dehors du fait que ces données sont pillées par des hackers avec une régularité métronomique (révélation sur les puces espion chinoises sur les cartes mères SuperMicro en octobre, 50 millions de comptes Facebook hackés en septembre...), la gigantesque collecte de données personnelles orchestrées par les géants du net débouche sur une méfiance croissante des utilisateurs.

Aux Etats-Unis, selon une étude du Pew Research Center, 26% des utilisateurs de Facebook âgés de plus de 18 ans ont ainsi supprimé l'application de leur smartphone au cours de l'année écoulée. Une proportion qui atteint même 44% chez les utilisateurs âgés de 18 à 29 ans. En

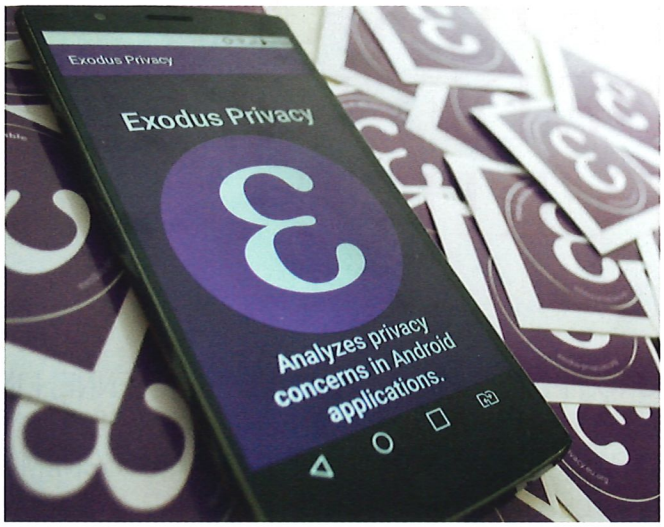
Des chercheurs ont montré qu'un téléphone Android – même inactif et immobile – se connecte 900 fois par jour avec les serveurs de Google

PHOTOS: DR

EXODUS PRIVACY PISTE LES PISTEURS

Parce qu'elle s'est rendu compte de la présence d'un pisteur (Teemo) destiné à collecter la géolocalisation de millions de personnes via des dizaines d'applications, l'hacktiviste U+039B publie sur le réseau social en logiciel libre Mastodon une alerte à ce sujet. Cela conduit à la création l'an dernier de l'association française Exodus Privacy. Ses membres s'emploient à rendre transparente la collecte de données sur smartphone. En plus d'une plateforme pour que n'importe qui puisse analyser ses applications, ils développent des outils qui rendent à la fois visibles ces pisteurs mais aussi les autorisations d'accès (aux micros, à la caméra...) noyées dans les conditions générales (sans compter l'accès aux applications installées qui ne nécessite aucune autorisation et permet de construire des marqueurs tels qu'orientation sexuelle, religion, opinion politique etc.).

«Les développeurs ajoutent ces pisteurs à leurs applis parce que c'est une source de monétisation au travers du ciblage publicitaire ou de la revente de données. Mais cela peut se faire aussi à leur insu lorsqu'ils ont recours à des bibliothèques de logiciels prêts à l'emploi qui contiennent ces pisteurs», explique MeTal_PoU, présidente d'Exodus Privacy. Depuis un an, les hacktivistes d'Exodus ont découverts 152 pisteurs différents dans 35 000 applications qui en contiennent de zéro jusqu'à trente parfois. Sans surprise, Google Ads est présente dans 42% des cas. Plus surprenant, l'application de Météo-France envoie ses données de géolocalisation des utilisateurs toutes les minutes à la régie pub de Facebook. Exodus fait cependant face à des limites: «ouvrir une application pour en lire le code est illégal, nous nous contentons de lire l'équivalent du sommaire de ces logiciels.» D'autre part, Exodus est limitée à Android parce que les applications de l'App Store sont protégées par des outils de gestion des droits numériques qui interdisent l'analyse.



Grâce à Exodus, tout utilisateur peut analyser ses applications.

Suisse, une étude de l'organisme de recherche Sotomo pour la Fondation Sanitas Assurance Maladie, rendue publique en juin dernier, révèle que plus de 70% des Helvètes désactivent certaines fonctions de leur smartphone comme la géolocalisation pour protéger leurs données personnelles.

Le problème que relève cependant le juriste spécialisé François Charlet, «c'est que même si vous refusez à une application d'ouvrir le GPS vous avez souvent déjà accepté le principe de la géolocalisation dans les conditions générales d'une app. Par conséquent, si le GPS est éteint, Facebook ou Google ne vous localisera pas par ce biais, mais il pourra le faire par d'autres moyens comme l'adresse IP du réseau wi-fi que vous utilisez.» «C'est truffé de pièges», confirme Karl Aberer.

Ce fouillis dans des conditions générales que personne ne lit – un groupe de défense de consommateurs australiens a demandé à un acteur de lire à haute voix celles du Kindle d'Amazon, soit 73 198 mots en 9 heures – a conduit l'Union européenne à mettre en place le RGPD entré en vigueur le 25 mai dernier. «C'est une Lex GAFAM avec des sanctions très lourdes puisque les amendes peuvent aller jusqu'à 4% du chiffre d'affaires mondial de l'entreprise», explique François Charlet.

Sur le papier, ce RGPD apporte des progrès significatifs: droit à l'accès et à l'effacement de ses données personnelles et surtout consentement explicite. Mais le diable est dans les détails. Comme l'explique Alexis Fitzjean O'Cobhthaigh à la Quadrature du Net, «l'article 7 du RGPD indique que le consentement est libre et pas subordonné à l'accès au service. Or, c'est exactement le contraire qui se passe. Les GAFAM vous refusent tout simplement l'accès à leurs services si vous ne consentez pas à leur donner accès à vos données personnelles.»

La Quadrature du Net a lancé une plainte collective contre les GAFAM à ce sujet. Pour courageuse et même fondée qu'elle soit, cette initiative fait face à un bulldozer. L'écosystème construit par les géants du net repose sur la moisson des données personnelles. C'est ce qui lui permet de prendre un par un des pans entiers d'activités économiques. De même que «le logiciel dévore le monde» selon le mot célèbre de l'inventeur des navigateurs web Marc Andreessen, la collecte des données personnelles concentre le pouvoir économique.

Après les médias, le commerce, le tourisme, le transport (Uber), l'hôtellerie (Airbnb), Amazon prépare maintenant son offensive dans la santé et Facebook dans la banque. Avec l'avantage du big data et tant pis si cela provoque la polarisation et la radicalisation des opinions. Dans la data economy, seuls les riches deviennent plus riches. ■

PHOTO: DR