Le Mémo – Épisode 5
Données personnelles : peut-on faire confiance à son téléphone ? 1/2

— Germain :

C’est une photo aérienne en noir et blanc. On reconnaît immédiatement ce bâtiment si emblématique des États-Unis... Le Pentagone. Quand on scrolle sur la page, l’image se couvre progressivement de centaines de points verts lumineux. Ils sont sur le parking et sur les routes qui y conduisent... sur les espaces verts... Mais surtout sur le bâtiment l’un des plus sécurisés du monde. Chacun de ces points, c’est un téléphone portable, dans une poche, dans une main, sur un bureau ou sur le tableau de bord d’une voiture. C’est une photographie exacte de l’emplacement où se trouvaient des centaines de personnes à une heure précise d’un jour précis de 2016.

Même constat, mêmes petits points verts, sur une plage de Los Angeles, dans le quartier de Wall Street, sur les collines de Beverly Hills, à Central Park.

En tout, les journalistes du New York Times ont récupéré 50 milliards de points de géolocalisation émis par 12 millions de téléphones. C’est la première fois que des journalistes accèdent à des jeux de données aussi massifs. Ils les ont récoltées grâce à une source anonyme... qui voulait alerter l’opinion publique sur un phénomène... nos téléphones, l’unique objet qu’on ne lâche jamais de la journée... sont localisés en permanence par des entreprises qui en ont fait leur spécialité.

[Identité sonore]

Bonjour Marine !

— Marine :

Bonjour Germain !

— Germain :

Bienvenue à tous dans le Mémo, le podcast qui décrypte pour vous les grands enjeux du numérique. Dans cet épisode, qui est le premier d’une mini-série sur le tracking via nos téléphones, on vous parle de la sécurité de vos données privées. Alors Marine, cette enquête du New York Times dont je viens de raconter quelques éléments, elle est glaçante... mais avant d’y revenir il faut bien comprendre de quoi on parle. Alors, la géolocalisation, ça marche comment ?

— Marine :

Ce qui est intéressant, et je le lis dans un article de ZDNet, c’est que des chercheurs de la Northeastern University de Boston ont démontré qu’on peut géolocaliser des téléphones, même lorsque le GPS (c’est le système mondial de positionnement par satellite) est désactivé. Pourquoi ? Parce que les téléphones sont dotés de capteurs : un accéléromètre, un magnétomètre, qui est une sorte de boussole et un gyroscope, qui permettent de déterminer l’orientation. Et surtout, ces

informations sont complétées grâce aux réseaux mobile et wifi. Si votre téléphone se connecte à une borne, il est très simple d'en connaître la localisation.

— Germain :

Et à quoi ça sert toutes ces fonctions ?

— Marine :

D'abord, ça vous sert à vous, à vous connecter aux réseaux mobiles. Mais aussi à vous repérer sur une carte pour choisir votre itinéraire. Mais en réalité, sur un smartphone, de très nombreuses applications utilisent les données de localisation. Votre application de météo par exemple, le navigateur web aussi... pour vous apporter un confort d'utilisation, des informations personnalisées. Vous pouvez d'ailleurs regarder dans les paramètres de votre téléphone quelles sont les applications qui ont l'autorisation d'accéder au GPS, c'est ce qu'explique un article de Bien vivre le digital.

— Germain :

Et certains acteurs n'ont pas hésité à développer de véritables mouchards qui reposent sur ces données...

— Marine :

Oui, ce sont ces applications proposées aux parents pour suivre leurs enfants. Un trackeur invisible dans le téléphone à suivre, une application sur le téléphone du parent et le voilà rassuré.
Mais on constate dans un article du Figaro que cet usage est parfois détourné, par des conjoints abusifs pour suivre leur épouse par exemple. « En 2018, le Centre Hubertine-Auclert a publié une enquête sur la cyberviolence. Sur les 302 victimes interrogées, 21% ont déclaré avoir été surveillées via des logiciels espions ou un autre dispositif de traçage. » Et là on ne parle bien sûr que de celles qui s'en sont rendu compte, or c'est très difficile à détecter. Ces pratiques sont punies par la loi : jusqu'à 45 000 € d'amende et un projet de loi devrait bientôt encore aggraver les peines encourues.

— Germain :

C'est rassurant ! On imagine vite que ces solutions peuvent être utilisées dans le cadre d'une surveillance plus massive …

— Marine :

Exactement, c'est ce qui se passe en Chine dans la région du Xinjiang. En arrivant, les gardes-frontière imposent à tout le monde, journalistes, touristes, etc. de leur laisser leur téléphone. Les journalistes du Guardian ont enquêté en partenariat avec d'autres médias… ils ont découvert que l'objectif, c'est d'installer une application cachée dans le téléphone, pour vérifier qu'il ne contient pas de document interdit, mais aussi probablement de géolocaliser les visiteurs.

— Germain :

Mais collecter les données de géolocalisation des individus, ça peut aussi être une pratique parfaitement légale…

— Marine :

Oui, et c’est justement sur cette pratique que le New York Times dont on parlait il y a un instant a enquêté. Les journalistes listent plusieurs entreprises qui en ont fait leur spécialité. Leur nom ne vous dira probablement rien, pourtant, l’une d’entre elles est forcément passée par votre téléphone. Ces entreprises collectent vos données de géolocalisation pour les revendre à des annonceurs qui peuvent alors vous proposer de la publicité contextualisée. D’ailleurs deux de ces entreprises sont françaises : Teemo et Fidzup. Ce qu’elles font est parfaitement légal. Elles proposent à des applications (comme celle qui vous donne la météo), d’installer un petit morceau de code qui collecte vos données de géolocalisation, en échange de revenus publicitaires. Elle revend ensuite les données à ses clients… Ces données ont évidemment beaucoup de valeur pour eux parce qu’en sachant, par exemple, que vous êtes déjà rentré dans leur magasin, ils peuvent vous envoyer de la publicité personnalisée.

— Germain :

Et donc ça, c’est légal.

— Marine :

Oui, parfaitement, parce que les fichiers sont anonymisés. L’entreprise de tracking n’envoie pas un tableau Excel avec vos nom, prénom, numéro de téléphone et localisation. Non, les données de tracking sont en réalité associées à un numéro de publicité, celui qui est attribué à votre téléphone (et que vous pouvez d’ailleurs changer régulièrement dans vos paramètres... pour remettre les compteurs à zéro).

— Germain :

Donc c’est l’anonymat des données qui rend la géolocalisation légale. Finalement, tant qu’on ne peut pas associer ces données à mon identité, il n’y a pas de problème.

— Marine :

Voilà. Sauf qu’en réalité, quand on relie ces points, on peut retracer des déplacements. Et ces déplacements sont uniques : mon domicile, mon travail, mes activités habituelles... Résultat, les journalistes du New York Times ont été capables de retracer les parcours d’individus comme un ingénieur chez Microsoft, qui d’ailleurs un jour s’est rendu dans les locaux d’Amazon… quelques semaines plus tard, il changeait de poste. Le fameux ingénieur a tout confirmé. Ils ont retracé aussi les parcours de journalistes d’investigation, de militaires, de policiers… donc ces données ne sont pas si anonymes et en cas d’attaque informatique, pourraient tomber entre de mauvaises mains.

— Germain :

Mais comment on fait pour passer d’une liste de points reliés entre eux à un individu ?

— Marine :

Des scientifiques ont mené une étude, en 2013, on peut retrouver le rapport sur le site de la revue scientifique Nature. Pendant 15 mois, ils ont collecté les données de localisation d'1 million et demi d'individus. Ils ont découvert qu'effectivement, la trace que nous laissons est unique. Plus encore qu'une empreinte digitale. En effet, là où il faut 12 points d'empreinte pour identifier une personne, il ne faut que 4 points de géolocalisation pour repérer 95 % des individus.

— Germain :

Et en Europe est-ce que le RGPD nous protège de ce type de pratiques ?

— Marine :

En tout cas, il nous offre plus de transparence. Le Règlement général pour la protection des données impose aux entreprises d'informer les utilisateurs avant d'exploiter les données à des fins de ciblage publicitaire, cela inclut donc la géolocalisation. Plusieurs entreprises, comme Fidzup ou Teemo, ont été épinglées pour leurs mauvaises pratiques en la matière. Mais la récolte et le partage des données de géolocalisation restent légaux si l'utilisateur est informé et qu'il a la possibilité de demander que toutes ces informations soient effacées, c'est ce que rappelle un article de Numérama.

— Germain :

Est-ce qu'on peut donner des conseils à nos auditeurs ? Comment peuvent-ils s'en protéger ?

— Marine :

Oui, la CNIL donne beaucoup de très bons conseils, on vous met le lien vers la page dans la description de l'épisode. Parmi ces conseils : désactiver l'autorisation de géolocalisation des applications qui n'en ont pas besoin (vous verrez, vous serez étonnés, moi par exemple, l'application qui me permet d'enregistrer du son était autorisée à me localiser). Ensuite, renouveler régulièrement votre identifiant publicitaire, pour couper le suivi de la géolocalisation, etc.
Bon, enfin la technologie n'est pas infaillible tout de même : au Danemark, 32 prisonniers ont été libérés fin 2019. Le motif ? De potentielles erreurs dans les données de géolocalisation qui avaient conduit à les suspecter. On peut lire toute l'histoire dans le Guardian.

— Germain :

Merci Marine et merci à tous, cet épisode était le premier de notre mini-série sur les données personnelles. Dans le prochain épisode, on se demandera si nos appareils électroniques nous écoutent ! En attendant, retrouvez tous les liens vers les ressources que nous avons utilisées pour ce podcast dans la description. On vous a aussi glissé quelques liens supplémentaires pour aller plus loin. N'hésitez pas à aller regarder et à très bientôt pour le prochain épisode du Mémo !

Sources :

- Twelve Million Phones, One Dataset, Zero Privacy (The New York Times)
- Comment le GPS peut vous pister, même lorsque vous l'éteignez (ZDNet)
- La géolocalisation sur mobile (Bien vivre le digital)
- Loi contre les violences conjugales: une mesure interdit l'espionnage du conjoint (Le Figaro)
- Chinese border guards put secret surveillance app on tourists' phones (The Guardian)
- Unique in the Crowd: The privacy bounds of human mobility (Nature)
- Les USA exposent enfin le pistage publicitaire non consenti sur les applications mobiles (Numérama)
- Denmark frees 32 inmates over flaws in phone geolocation evidence (The Guardian)
- Maîtrisez les réglages « vie privée » de votre smartphone (CNIL)