Géolocalisation

Source
Wikipédia
« Géolocalisation »

La **géolocalisation** est un procédé permettant de positionner un objet, un véhicule, ou une personne sur un plan ou une carte à l'aide de ses coordonnées géographiques. Certains systèmes permettent également de connaître l'altitude.

Les applications de la géolocalisation sont en plein développement, tant sur le plan privé que sur le plan professionnel. De plus, couplées à des systèmes de télérelève intégrés et sur mesure, de vraies applications métier ont rapidement vu le jour.

Applications professionnelles

La géolocalisation dans le milieu professionnel est presque toujours synonyme de gain de productivité, d'économies de carburant, d'économies de communications et de sécurité accrue. De plus, ces solutions offrent aux responsables de l'exploitation du parc une vision globale et un meilleur temps de réactivité en cas d'incident. Cela permet à l'entreprise utilisant un système de géolocalisation d'améliorer son service client et de réduire ses coûts afin d'accroître sa compétitivité.

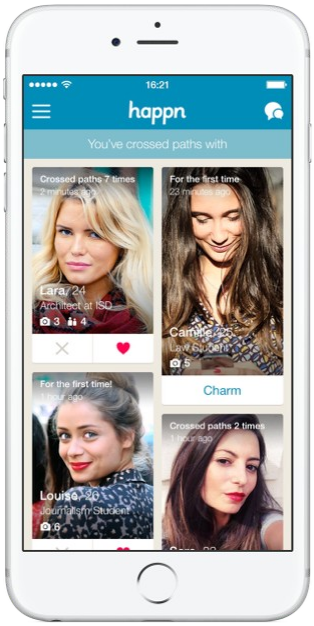
Quelques domaines dans lesquels la géolocalisation est communément utilisée sont listés ci-dessous :

- transport de marchandises et logistique ;
- propreté urbaine et assainissement ;
- transport de passagers ;
- analyse du trafic routier ;
- suivi et protection de personnes ;
- protection de marchandises, véhicules et antivol ;
- suivi de rallyes en désert ;
- suivi et protection des convois humanitaires ;
- études comportementales (par exemple, comprendre la diffusion d'une maladie localisée en observant les mouvements d'une population restreinte) ;
- suivi des véhicules par les assureurs (cela permet de calculer les facteurs de risque de l'utilisateur ou de facturer l'utilisateur en fonction du nombre de kilomètres parcourus) ;
- étude de l'habitat et des déplacements de mammifères difficilement observables, dont les individus sont équipés de colliers émetteurs, en écologie ou biologie des populations (par exemple, suivi de la population d'ours bruns dans les Pyrénées) ;
- etc.

Source
01net.com
8 juillet 2016

1. Comment les utilisateurs de Tinder ou Happn peuvent être suivis (presque) à la trace

Des chercheurs en sécurité ont montré qu'il était possible de suivre les déplacements des utilisateurs d'une application de rencontre géolocalisée, simplement en s'appuyant sur les notifications de présence. Explications.



Happn, Tinder, Grinder,… Les applications de rencontres géolocalisées sont fun et ont le vent en poupe. Pourtant, elles ne sont pas vraiment sans risque pour notre vie privée. Par définition, ces applications envoient en permanence notre localisation pour trouver l'âme sœur. Évidemment, seuls les serveurs de l'application reçoivent ces données, pas les autres participants. Un tiers ne peut donc pas suivre quelqu'un à la trace… en théorie du moins. Car avec quelques bonnes idées et un peu de programmation, il s'avère que c'est tout à fait possible.

La démonstration a été fournie samedi 2 juillet, à l'occasion de la conférence Nuit du Hack 2016. Julien Legras et Julien Szlamowicz, deux chercheurs en sécurité de la société Synacktiv, ont développé un logiciel permettant de détecter la présence d'une personne dans une zone donnée et de surveiller ses déplacements. Comment ? En déployant sur cette zone une grille d'agents-utilisateurs qui correspondent aux désirs de rencontre de la personne ciblée, ce qui activera les notifications de présence.

En réalité, ces agents sont totalement virtuels. Pour les créer, il faut avoir une série de comptes Facebook, ce qui n'est pas insurmontable. Ici, les deux chercheurs on utilisé une quinzaine de comptes Facebook pour créer ces faux utilisateurs. Le logiciel se contente alors d'envoyer des requêtes de positionnement aux serveurs de l'application pour donner l'impression qu'ils se trouvent réellement sur ces lieux. Ensuite, il suffit d'attendre que la cible passe à proximité de l'un ou plusieurs de ces agents (250 m pour l'application Happn par exemple) pour qu'elle soit prise dans ce filet de surveillance improvisé. Et la traque peut commencer.

La localisation n'est pas forcément très précise, vu le rayon d'action de l'application. Mais si la cible est repérée par trois agents en même temps, la zone peut alors être circonscrite à l'intersection de trois cercles, c'est-à-dire l'équivalent d'un petit triangle équilatéral de 13 mètres (dans le cas de l'application Happn par exemple). Quand la cible est détectée, le logiciel va ensuite décaler la grille d'agents en permanence pour centrer la cible sur ce petit triangle et, ainsi, pouvoir la suivre avec une certaine précision.

La création de ce système de surveillance n'aura nécessité que quelques jours. « Il nous a fallu un peu moins de deux jours pour coder l'application, précise Julien Szlamowicz. Le plus long a ensuite été de créer une quinzaine d'agents (création de comptes Facebook puis activation dans l'application). Il nous a fallu pour cela une petite partie de la matinée suivante. »

Évidemment, cette technique a aussi ses limites. Elle est bien adaptée pour surveiller un quartier ou un parc, mais pas tellement au-delà. Pour couvrir Paris, par exemple, il faudrait un millier d'agents, ce qui commence à faire beaucoup. Et pour couvrir la France, il en faudrait plusieurs millions, ce qui est totalement hors de portée. Et ce n'est pas plus mal.

Source
L'Express
Juliette Pousson
26 juin 2017

2. Localisation sur Snapchat : des associations de protection de l'enfance inquiètes

L'application très utilisée par les adolescents permet désormais à deux personnes "amies" de se géolocaliser. Une fonctionnalité qui effraie les autorités.

« Donc Snapchat Map est devenu un nouveau moyen pour les pédophiles de traquer leurs proies si je comprends bien ? », s'alarme un internaute sur Twitter. Lancée mercredi dernier via une mise à

jour de l'application, la nouvelle fonctionnalité de Snapchat fait déjà polémique.

L'appli utilise désormais un outil de géolocalisation en temps réel, qui permet de savoir où sont précisément situés ses amis. Ces derniers peuvent en retour savoir où l'on se trouve. Pour apercevoir la carte, il suffit d'effectuer un petit zoom arrière depuis l'écran principal de son application. Les avatars de vos amis apparaissent alors. Pratique, certes, mais également dangereux jugent plusieurs associations.

Selon le site *The Verge*, la Snap Map pose un vrai problème de respect de la vie privée. « Quand j'ai allumé Snap Map, j'ai vu le Bitmoji [l'avatar] d'une de mes amis dans une zone résidentielle. J'ai supposé que c'était sa maison », écrit le journaliste. « Il s'avère qu'elle ne savait pas que Snap Map était activé, ni qu'elle montrait sa localisation à chaque fois qu'elle ouvrait l'appli », ajoute-t-il.

Il suffit en effet de prendre une photo via Snapchat, sans même avoir l'intention de la poster, pour que l'application géolocalise l'utilisateur, indique Slate. « Parce que Snap Map montre exactement où vous vous trouvez à chaque fois que vous ouvrez l'appli, un nombre important de scénarios pourrait se produire sans même qu'un utilisateur publie des snaps de façon publique », estime *The Verge*.

Snapchat pourrait dès lors être utilisé pour traquer des personnes, savoir précisément où elles vivent, travaillent et mangent, s'inquiètent certains parents. Au Royaume-Uni, l'association *Childnet* encourage les utilisateurs à ne pas partager leur localisation, particulièrement avec des gens qu'elles ne connaissent pas en personne, souligne *Le Monde*.

« C'est inquiétant que Snapchat permette à des moins de 18 ans de diffuser leur localisation sur une application où elle peut être accessible par toute personnes faisant partie des contacts », renchérit la National society for the prevention of cruelty to children (NSPCC) dans *The Telegraph*.

La police de Nouvelle-Zélande a publié un avertissement sur sa page Facebook. « Si vous ou votre enfant êtes un utilisateur Snapchat, vous devriez régler rapidement vos paramètres », prévient-elle. La police de Preston, au nord de Liverpool, a également publié un message Facebook dans lequel elle explique comment désactiver la fonctionnalité Snap Map.

Source
lexpress.fr
22 février 2018

3. Des espions de la DGSE identifiés à cause de l'appli sportive Strava

L'application, qui géolocalise les parcours des courses de ses utilisateurs, a permis d'identifier des espions français, leur lieu de travail et leurs planques en opération.

L'état-major français des armées avait déjà pris le « problème Strava » au sérieux, mais il n'avait peut-être pas mesuré l'étendue des dégâts. En janvier dernier, les cartes issues des données de l'application de course à pied ou vélo, Strava, qui permet notamment de géolocaliser les courses des joggeurs, ont été mises en ligne. Depuis, ces données ont révélé que des soldats américains en zone de conflit, mais aussi des soldats français, faisaient leurs footings autour de leurs bases, parfois secrètes, révélant ainsi leur position.

L'armée française, si elle s'était montrée rassurante en affirmant « qu'aucune installation secrète n'a été révélée », avait tout de même rappelé à ses soldats imprudents que la « désactivation des fonctions de géolocalisation et de GPS » était une règle de sécurité élémentaire. Mais selon le *Canard enchaîné*, dans son édition du 21 février, l'état-major n'a apparemment pas été assez clair.

Certains militaires auraient choisi d'ignorer ces avertissements. Parmi eux, certains agents de la très secrète Direction générale de la Sécurité extérieure (DGSE), qui ont pu être identifiés et suivis à la trace, rapporte l'hebdomadaire satirique. « Certains espions sont benoîtement restés branchés » après les avertissements du ministère de la Défense, et « vu les tracés cartographiques ultra-précis de l'application, il était alors facile de repérer les joggeurs qui, le midi, quittaient et regagnaient en petites foulées des sites appartenant à la DGSE », écrit le *Canard*.

Et si ces espions ont cru qu'utiliser un pseudo sur Strava protégerait, ils ont fait preuve d'une naïveté incompréhensible de la part d'agents dont la paranoïa est normalement un art. Comme l'explique l'hebdomadaire, certains enregistraient tous leurs footings, même ceux accomplis lors de compétitions officielles, comme le marathon de Paris, auxquelles ils s'inscrivaient sous... leur vrai nom.

Et comme les résultats de ces épreuves sont disponibles sur Internet, il suffisait de les comparer avec les données publiques de Strava pour découvrir qui se cache derrière quel pseudo. « Ce n'est pas Le bureau des légendes, mais OSS 117 », se moque *Le Canard Enchaîné*, qui a pu identifier « un agent qui a pris comme couverture le nom d'un personnage de dessin animé ».

Grâce à l'exploitation des informations laissées en ligne -notamment sur Facebook- sous son vrai nom et ses informations géolocalisées laissées en ligne par Strava, les journalistes du *Canard* ont pu reconstituer « l'environnement familial et professionnel » de cet espion imprudent. L'identité de sa femme, très loquace sur Facebook, a été trouvée, le footing autour du domicile de sa mère a permis d'identifier son adresse, comme ceux effectués le week-end à laisser deviner son domicile en Île-de-France.

Pire encore, l'agent en question, visiblement avide de suivre ses performances sportives en toutes circonstances, s'est servi de son application Strava alors qu'il était en mission en Irak. « Un mois durant, sa planque dans un bâtiment en Irak était aisément géo-localisable », alerte l'hebdomadaire. Heureusement pour lui, les terroristes de Daech n'ont apparemment pas été aussi assidus que le *Canard*.

Source
Usbek & Rica
Annabelle Laurent
17 avril 2019

4. Les données de Google sont devenues une mine d'or pour la police américaine

La police américaine adresse de plus en plus de requêtes à Google pour géolocaliser des suspects en accédant à une base de données qui contient les positions géographiques de centaines de millions de téléphones dans le monde, a révélé le New York Times. La méthode est critiquée.

Le recours à cette technique d'investigation, utilisée pour la première fois en 2016, a « *fortement augmenté* » ces six derniers mois, assurent les employés de Google interrogés par le *New York Times*. Un salarié parle d'un record de 180 requêtes comptabilisées en une seule semaine. Google refuse de commenter ces chiffres. Que lui demande exactement la police ? Un mandat pour avoir accès à une gigantesque base de données qui contient la position géographique précise de plusieurs centaines de millions d'appareils dans le monde depuis près de dix ans. Google, l'appelle, en interne, « Sensorvault ».

La police indique une zone géographique et une période de temps, Google lui fournit la liste de tous les appareils présents au moment et au lieu indiqués. Une fois que la police a enquêté et réduit son champ de recherches à quelques appareils, Google révèle les noms et adresses mail de leurs propriétaires. Et ce au risque d'arrêter des innocents, s'inquiète le *New York Times*.

Le quotidien raconte l'histoire de Jorge Molina, arrêté fin décembre dans le cadre d'une enquête pour meurtre. La police l'informe que les données de son téléphone indiquent qu'il était présent à l'endroit où un homme a été assassiné neuf mois plus tôt. Les enquêteurs disaient également avoir une autre élément à charge : une vidéo de sécurité montrant quelqu'un en train de tirer depuis une Honda Civic blanche, le modèle de la voiture de Jorge Molina. Mais celui-ci passe une semaine en prison, avant d'être relâché : entre temps la police avait arrêté un autre suspect, une des connaissances de Jorge Molina, qui utilisait parfois sa voiture...

Des inquiétudes sur le plan légal

« *Ce cas démontre les promesses et les dangers de cette nouvelle technique d'investigation »,* note le *New York Times*. D'autant que tous les États ne garantissent pas l'anonymat des informations obtenues via cette méthode. Orin Kerr, professeur de droit à l'Université de Californie et spécialisé dans la question des enquêtes criminelles à l'ère numérique, s'inquiète ainsi de dérives légales sur ce sujet. Dans le Minnesota, le nom d'un homme innocent repéré comme un potentiel suspect via cette méthode (son téléphone portable avait été repéré à proximité d'un cambriolage) a été donné à un journaliste. L'homme, chauffeur de taxi, s'est étonné que ses données de géolocalisation aient été révélées : « *Avec mon taxi, je conduis partout*. »

Ces recherches posent par ailleurs une question constitutionnelle, car le quatrième amendement stipule qu'un mandat doit avoir une portée limitée et établir des motifs probables et suffisants. Or, le mandat demandé à Google peut parfois concerner des zones et des plages horaires étendues, ou même s'éloigner de la demande initiale jusqu'à « *offrir un portrait précis des habitudes d'un individu* ». Enfin, Google ne dispose pas des données de tous les appareils - les données de géolocalisation peuvent être désactivées - sa vue est donc biaisée, et incomplète.

« *Nous n'allons pas accuser n'importe qui juste parce que Google nous a dit qu'il était sur le lieu du crime* », tempère Gary Ernsdorff, un procureur de l'État de Washington qui a travaillé sur des affaires impliquant les données de géolocalisation fournies par Google.

Les révélations du *New York Times* sur Sensorvault rappellent les nombreuses questions éthiques

et légales posées par les requêtes de la police ou de la justice, toujours plus nombreuses, faites aux entreprises de la tech. On se souvient d'Amazon qui, en 2016, s'était refusée à donner à la justice américaine les enregistrements de l'enceinte connectée d'un homme accusé d'avoir tué un de ses amis. L'homme avait finalement clamé son innocence et autorisé Amazon à fournir les données réclamées, et les charges contre lui avaient été abandonnées.

Les entreprises de la tech ne sont pas les seules à intéresser la police. Les bases de données des plateformes proposant des tests ADN dits « récréatifs » suscitent également la convoitise du FBI. Pendant l'été 2018, les quatre entreprises dominant le secteur avaient toutes promis qu'elle ne laisseraient pas la police entrer dans leurs bases de données sans mandat, mais quelques semaines plus tard, « *Family Tree DNA autorisait déjà le FBI à télécharger l'ADN récupéré sur des cadavres et des tâches de sang et à naviguer dans la base de données comme n'importe quel client, en regardant les noms et les relations entre les utilisateurs.* »

Source
lebigdata.fr
Bastien L
23 décembre 2019

5. Votre smartphone permet de vous suivre à la trace grâce aux données GPS

Un ensemble de données découvert par le New York Times contient plus de 50 milliards de pings de géolocalisation collectés par les smartphones. Ces données permettent de surveiller les déplacements de 12 millions d'Américains, et prouvent que nos téléphones sont de véritables traceurs de poche…

Votre smartphone permet de vous suivre à la trace. C'est ce que révèle (ou confirme) le *New York Times,* qui vient de mettre la main sur un dataset en fuite contenant les données de géolocalisation de 12 millions d'Américains.

Au total, cet ensemble de données rassemble 50 milliards de « ping » de géolocalisation. Ces pings permettent d'observer avec précision les déplacements de millions de smartphones dans plusieurs grandes villes américaines telles que Washington, New York, San Francisco et Los Angeles.

En analysant ce fichier qui lui a été fourni, le *Times* a découvert que ces données pouvaient être utilisées pour révéler nos secrets les plus intimes. Bien qu'elles soient anonymisées, il est aisé d'identifier le possesseur d'un smartphone ne serait-ce qu'en inspectant les déplacements vers son domicile ou son travail.

Après avoir déterminé quel lieu sert de domicile à la personne, il suffit de rechercher le propriétaire d'une adresse sur internet pour l'identifier. C'est ainsi que le NYT a pu suivre les déplacements d'officiers militaires, repérer les écoles des enfants d'hommes politiques où vérifier où partent en vacances des avocats de renom. Même Donald Trump a pu être pisté par les journalistes.

Les données ont même permis de révéler d'embarrassants secrets, comme des visites répétées dans des motels pour quelques heures. Cependant, le journal n'a cité aucun nom sans consentement explicite.

Les données de géolocalisation de smartphones : une véritable industrie

Même si la plupart des utilisateurs savent que les applications de leurs smartphones utilisent leurs données de géolocalisation, peu d'entre eux s'imaginent dans quelle mesure ces données sont collectées, stockées... mais aussi revendues.

L'échange de données de géolocalisation est devenu une véritable industrie, reposant sur le traçage de chaque américain au quotidien. Les publicitaires, notamment, s'intéressent particulièrement à ces informations. Elles peuvent être exploitées pour proposer des publicités mobiles ciblées, où même pour vérifier l'efficacité des panneaux publicitaires en vérifiant si ceux qui les voient passent à l'achat...

Il est aussi fréquent que vos données de géolocalisation soient collectées et revendues avec votre identifiant de publicité mobile. Or, cet identifiant peut permettre de remonter à d'autres informations personnelles telles que votre adresse email, votre numéro de téléphone ou même votre réseau WiFi domestique.

L'anonymisation des données est donc une vaste fumisterie, comme l'avait déjà révélé le *New York Times* en juillet 2019 à l'issue d'une vaste enquête. Malheureusement, en dépit des risques que représente ce trafic de données pour la confidentialité, cette industrie est très peu réglementée.

Les entreprises et groupes industriels bénéficient donc d'une liberté presque absolue dans ce

domaine. Rien ne leur interdit de collecter les données ni de les partager comme elles le souhaitent.

Même si cet ensemble de données spécifique contient uniquement des informations sur une partie de la population américaine, il ne fait aucun doute qu'il existe une multitude de datasets similaires. On peut donc bel et bien partir du principe que nos smartphones sont exploités pour nous épier en permanence…

Source
Futura
Edward Back
8 avril 2021

6. Votre smartphone vous espionne à votre insu et c'est effrayant

Une nouvelle étude s'est intéressée à la quantité d'informations collectées par les smartphones. En utilisant uniquement la géolocalisation, deux chercheurs ont pu découvrir des informations comme l'état de santé, la religion et même l'ethnicité des utilisateurs.

Jeux en réalité virtuelle, applis de rencontres, de cartographie, de météo... Toutes ces applications mobiles demandent l'accès à vos données de localisation, mais elles collectent en réalité bien plus d'informations. Deux chercheurs, de l'université de Bologne et de l'*University College* de Londres, viennent de publier une étude s'intéressant aux informations privées des utilisateurs qu'il est possible d'inférer uniquement grâce à la géolocalisation.

Un groupe de 69 volontaires a installé une application nommée TrackAdvisor qui piste leurs déplacements et créée spécialement pour l'étude. Elle a collecté plus de 200.000 localisations dans 2.500 lieux. TrackAdvisor a ainsi pu inférer plus de 5.000 informations personnelles. Les volontaires pouvaient noter si ces inférences étaient justes et relevaient de la vie privée. Les chercheurs ont découvert de nombreuses informations notamment sur la santé, la situation socio-économique, l'ethnicité et la religion des participants.

L'intelligence artificielle pour analyser les données

« *Grâce aux techniques d'apprentissage automatique, ces données fournissent des informations sensibles comme le domicile des utilisateurs, leurs habitudes, ce qui les intéresse, leurs données démographiques et des informations sur la personnalité des utilisateurs* » a précisé le chercheur italien Mateo Benni.

Il s'agit de la première étude de cette ampleur. En 2019, le site Kotaku s'était intéressé aux données de 10 volontaires collectées par Niantic, développeur de jeux mobiles de réalité augmentée comme Pokémon Go. Leurs conclusions étaient alors similaires, mais cette nouvelle étude est beaucoup plus précise, notamment grâce à l'intelligence artificielle. Pour contrer cette invasion dans la vie privée, les chercheurs imaginent un système conçu pour alerter les utilisateurs lorsqu'ils se rendent dans des lieux comme des hôpitaux, ou qui bloque la collecte de données depuis les tiers.

Source
Vice.com
Sebastian Meineck
20 novembre 2020

7. Six bonnes raisons de ne plus utiliser Google Maps

Avec un milliard d'utilisateurs actifs par mois, Google Maps sait tout. Non seulement les noms de toutes les rues, cafés, bars et magasins, mais aussi les endroits où les gens se rendent. Mais s'il a le pouvoir de suivre chacun de nos pas, cela ne veut pas forcément dire qu'il abuse de ce pouvoir. Mais il pourrait le faire s'il le voulait, ce qui est un problème en soi, d'autant plus que le siège de Google se trouve aux États-Unis, où la législation sur la vie privée est moins stricte qu'en Europe et où les agences de renseignement ont l'habitude de surveiller les particuliers (on vous voit, la NSA).

Oui, Google Maps est incroyablement utile. Mais voici quelques raisons qui vous inciteront à vérifier vos paramètres de confidentialité et à vous demander quelle quantité de données personnelles vous êtes prêt à sacrifier au nom de la commodité.

Google Maps veut accéder à l'historique de vos recherches

Dans les paramètres, il est dit que l'option « Activité sur le Web et les applications » permet à l'utilisateur de bénéficier d'une expérience plus rapide et plus personnalisée. En clair, cela signifie que chaque endroit que vous consultez dans l'application – qu'il s'agisse d'un club de strip-tease, d'un kebab ou de la localisation de votre dealer – est enregistré et intégré dans l'algorithme du moteur de recherche de Google pendant une période de 18 mois.

Google sait bien que tout cela est un peu flippant. C'est pourquoi l'entreprise utilise des dark

patterns, c'est-à-dire des interfaces utilisateur conçues pour nous tromper ou nous manipuler, par exemple en mettant en évidence une option avec certaines polices ou des couleurs plus vives.

Nous avons donc créé un nouveau compte Google pour tenter de repérer ces dark patterns. Après avoir cliqué sur « Créer un compte », une fenêtre pop-up nous indique que le compte est « configuré pour inclure des fonctions de personnalisation » en petites lettres grises. En cliquant sur « Confirmer », nous acceptons d'activer l'option « Activité sur le Web et les applications » mentionnée ci-dessus. L'autre bouton, « Plus d'options », est moins visible et redirige vers une nouvelle page avec des explications denses et compliquées. Nous devons désactiver l'option manuellement.

Google Maps limite ses fonctionnalités si vous ne partagez pas votre historique de recherche

Si vous ouvrez l'application Google Maps, vous verrez un cercle avec votre photo de profil dans le coin supérieur droit qui indique que vous êtes connecté à votre compte Google. Ce n'est pas nécessaire, et il vous suffit de vous déconnecter. Évidemment, le bouton pour se déconnecter de votre compte est légèrement caché, mais vous pouvez le trouver comme ceci : cliquez sur le cercle > Paramètres > faites défiler vers le bas > Se déconnecter de Google Maps.

Google Maps peut vous balancer

Autre fonctionnalité problématique : « Vos trajets Google Maps » qui « affiche une estimation des lieux que vous avez visités et des itinéraires que vous avez empruntés d'après l'historique de vos positions. » Cette fonction vous permet de consulter les informations figurant dans vos trajets, y compris les modes de transports utilisés, comme en voiture ou à vélo. L'inconvénient, bien sûr, est que tous vos déplacements sont connus de Google et de toute personne ayant accès à votre compte.

Et il n'y a pas seulement les hackers dont vous devez vous méfier ; Google peut aussi fournir vos données à des agences gouvernementales comme la police. Sur sa page FAQ à ce sujet, Google indique que son équipe juridique évalue chaque cas individuellement. Tous les six mois, l'entreprise publie un rapport de transparence, mais rien n'est disponible pour 2020. Entre juillet et décembre 2019, Google a reçu 81 785 demandes de divulgation d'informations concernant 175 715 comptes dans le monde entier et a répondu favorablement à 74 % d'entre elles.

Si votre « historique des positions » est activé, votre téléphone « indique les positions des appareils sur lesquels vous êtes connecté à votre compte ». Cette fonction est utile si vous perdez votre téléphone, mais elle en fait surtout un véritable dispositif de suivi.

Google Maps veut connaître vos habitudes

Les avis Google peuvent être très utiles, mais une recherche rapide peut révéler des informations sensibles que les utilisateurs ont oubliées par inadvertance. Un exemple est celui d'un utilisateur (qui semble utiliser son vrai nom) qui a écrit la critique suivante sur un supermarché à Berlin : « Depuis quatre ans, j'y vais deux ou trois fois par semaine pour faire les courses pour ma famille. » Il va sans dire que le fait de partager ce type d'informations avec tout le monde peut être risqué.

Google Maps demande souvent aux utilisateurs de partager une évaluation publique rapide. « Comment était le Berlin Burger ? », demande l'application après votre dîner. Cette question a priori désinvolte et légère donne l'impression d'aider les autres, mais toutes ces informations sont stockées sur votre profil Google et toute personne qui le lira pourra facilement savoir si vous avez été quelque part pendant une courte période (par exemple en vacances) ou si vous vivez à proximité.

Si vous finissez par regretter un avis, Google vous donne au moins la possibilité de le rendre privé après l'avoir publié. Pour ce faire : Photo de profil > Modifier le profil > Profil et confidentialité > Faites défiler vers le bas > Profil limité. Si vous activez cette option, vous devrez approuver les personnes qui peuvent suivre votre profil et voir vos avis.

Google Maps n'aime pas que vous soyez déconnecté

Vous vous souvenez de la navigation GPS ? Elle était peut-être maladroite et lente, mais il n'était pas nécessaire d'être connecté à Internet pour être dirigé. En fait, d'autres applications offrent une navigation sans connexion Internet. Dans l'application Google, vous pouvez télécharger les cartes, mais la navigation hors ligne n'est disponible que pour les voitures. Il semble assez improbable que le géant de la technologie ne soit pas en mesure de guider les piétons et les cyclistes sans Internet.

Google donne l'impression que tout cela est pour votre bien

« La mission de Google consiste à proposer des expériences utiles et enrichissantes, pour lesquelles les données de localisation jouent un rôle essentiel », explique l'entreprise sur son site. Elle utilise ces données pour toutes sortes de choses utiles, comme la « sécurité » ou les « paramètres linguistiques ». Et, bien sûr, pour vendre des annonces. Google offre également aux annonceurs la possibilité de « mesurer le degré de notoriété de leur marque ».

Parfois, il existe de bonnes alternatives aux applications problématiques. C'est vrai pour WhatsApp, par exemple, mais pas pour Google Maps. Apple Maps a une politique de confidentialité plus stricte, mais elle n'est pas disponible pour Android. Des applications comme Here WeGo collectent aussi des données et ne sont pas aussi bonnes, mais si vous êtes un marcheur qui préfère rester hors ligne, OsmAnd et Maps.me peuvent au moins vous montrer le chemin sans passer par Internet.

Source
Korii
Antoine Hasday
26 mars 2020

8. Les outils de surveillance utilisés contre la Covid-19 lui survivront

Milo Hsieh, journaliste basé à Taïwan, a eu la mauvaise idée d'oublier de charger son téléphone portable durant sa quarantaine. À 7h30 du matin, le portable s'est éteint. Cinquante minutes plus tard, la police frappait à sa porte.

Sur l'île, les autorités géolocalisent les personnes en quarantaine grâce à leurs téléphones portables, pour s'assurer qu'elles ne sortent pas de chez elles. Toute anomalie déclenche une alerte.

À Singapour, pour faire respecter la quarantaine, les autorités envoient plusieurs SMS par jour aux habitant·es en leur demandant de partager leurs coordonnées GPS.

Par ailleurs, l'ensemble de la population a été invitée à télécharger une application baptisée TraceTogether. Celle-ci a accès à l'ensemble des contacts du téléphone et active le Bluetooth.

L'application enregistre les contacts entre les personnes. Si quelqu'un contracte le coronavirus, toutes ses interactions seront ainsi connues. Cela permet de faire du « *contact tracing»* –retracer tous les contacts d'une personne contaminée sur les quinze derniers jours– beaucoup plus facilement et sûrement. Des informations sur les personnes contaminées sont également disponibles sur internet (!).

En Corée du Sud, des technologies intrusives sont aussi utilisées pour suivre la progression de la maladie au sein de la population et faire respecter les quarantaines.

En Occident aussi

La tolérance à la surveillance semble plus importante dans les démocraties asiatiques –à l'exception peut-être de Hong Kong– que dans les pays européens. Certaines solutions technologiques qui y sont mises en œuvre seraient plus difficilement acceptées dans l'UE. Néanmoins, des formes similaires de surveillance pointent déjà le bout de leur nez en Europe et aux États-Unis.

Dans une tribune publiée sur Fast Company, deux chercheurs ont appelé les pays occidentaux à utiliser la géolocalisation des téléphones portables pour combattre l'épidémie.

En France, un amendement déposé par deux sénateurs LR le 19 mars proposait que *« toute mesure visant à permettre la collecte et le traitement de données de santé et de localisation* [soit] *autorisée pendant une durée de six mois».* Il a été rejeté. Quelques jours plus tard, l'Élysée faisait pourtant l'annonce suivante.

La société américaine Athena Security s'est fait connaître en commercialisant des caméras thermiques intelligentes, qui peuvent détecter les armes à feu.

À présent, elle veut les utiliser pour détecter les personnes contaminées par le Covid-19. Cela permettrait de surveiller le risque de contamination dans des endroits qui restent peuplés en période de quarantaine. La technologie d'Athena Security doit notamment être installée dans plusieurs aéroports américains.

« Effet cliquet »

Il est probable que certaines de ces technologies de surveillance puissent aider à combattre la pandémie. L'utilisation des données de localisation des téléphones est un moyen très efficace de faire du « *contact tracing* ».

Toute solution technologique permettant de s'assurer que la quarantaine est respectée est utile. Des caméras thermiques pourraient permettre d'alerter dès les premiers signes de recrudescence de l'épidémie. Le problème, c'est qu'il sera difficile de revenir en arrière une fois l'épidémie passée.

« Le consensus scientifique qui se dégage, c'est qu'il faut tester massivement et tracer –c'est la stratégie sud-coréenne en quelque sorte, qui est très intrusive. Cette pandémie anesthésie encore un peu plus notre vigilance vis-à-vis des dispositifs menaçant les libertés. L'affrontement classique entre les défenseurs des libertés et les gouvernements qui les rognent vole un peu en éclats. On est face à un dilemme éthique incroyable, il va falloir trouver le bon équilibre », analyse Olivier Tesquet, journaliste à Télérama et auteur de *À la trace – Enquête sur les nouveaux territoires de la surveillance* (Premier Parallèle, 2020).

Si l'on installe des caméras thermiques dans les aéroports et les gares, elles risquent de rester indéfinement pour rentabiliser le coût de l'investissement.

Si les autorités sanitaires ont accès aux données de localisation des citoyen·nes, elles risquent de vouloir conserver cet accès pour éviter tout retour de l'épidémie. Si l'utilisation de drones pour la gestion de foules se montre efficace, pourquoi ne pas la développer, par exemple, en manifestation ?

« Il y a un effet cliquet assez net, je crains qu'un on ait du mal à abandonner un certain nombre de ces technologies [comme avec les mesures “d'exception” prises depuis 2015 face au terrorisme]. *Les dispositifs techniques sont une forme de fuite en avant : ce sont des instruments pour gouverner en temps de crise, mais comme depuis 2015 on a passé plus de temps en crise* [qu'en période “normale”]*, l'exception devient en quelque sorte la norme. Un instrument prévu pour des finalités particulières devient permanent. D'autant plus que l'épidémie va probablement durer et que les mesures d'exception ne seront pas levées d'un coup »*, poursuit Olivier Tesquet.

Il est donc important que le bénéfice en matière de santé publique apporté par chacune de ces technologies soit mis en balance avec son impact sur les libertés publiques. Une surveillance généralisée porterait une atteinte inacceptable à nos droits sans forcément garantir notre sécurité.

Source
letemps.ch
Chams Iaz
5 septembre 2021

9. En Australie, selfies et vidéos en direct deviennent des outils de surveillance des personnes en quarantaine

Vous avez été mis en quarantaine ? Vous avez quinze minutes pour vous connecter à l'application de l'État d'Australie méridionale et prouver que vous êtes bien chez vous, grâce à la reconnaissance faciale et la géolocalisation. Un dispositif orwellien qui pourrait être déployé au niveau national.

Pour s′assurer du respect des mesures de quarantaine imposées dans le pays, un État australien impose à ses citoyens de se plier à un contrôle atypique : une application développée par le gouvernement, Home Quarantine SA, doit être installée pour vérifier que chacun et chacune se trouve bien en isolement à l'adresse indiquée.

Souriez, vous êtes filmé

La personne contrôlée est contactée par SMS, de manière aléatoire, et dispose de quinze minutes pour montrer son visage devant la caméra de son smartphone. La date, l'heure et sa localisation sont alors vérifiées. Cela pour prouver que le sujet filmé en direct est bien à son domicile. Mais ce n'est pas tout : ses traits sont également scrutés par un logiciel de reconnaissance faciale afin de déterminer s'ils correspondent bien au profil de la personne enregistrée.

En cas d'échec, dû à des difficultés technologiques ou à un défaut de notification, la personne est immédiatement contactée par téléphone et doit se justifier. Si elle manque cet appel, un agent de la police locale se rendra à son domicile pour procéder à un contrôle. Selon les directives, les personnes qui enfreignent la quarantaine peuvent encourir une amende allant jusqu'à 1000 dollars australiens (680 CHF).

Pour le Département de la santé, doivent se plier à cet exercice toutes les personnes susceptibles d'avoir été en contact avec un individu ayant le Covid-19 ou qui « entrent dans un État, territoire ou zone qui impose une quarantaine ». Pour rappel, l'Australie a sévèrement restreint les déplacements entre ses six Etats et ses résidents sont contraints de passer quatorze jours en quarantaine à leur retour. Dès le début de la pandémie, une quarantaine hôtelière a été imposée pour les voyageurs internationaux. Elle s'applique désormais aux Australiens.

La plupart de ceux passés dans une zone potentiellement contaminée sont alors hébergés, à leurs frais, dans des chambres d'hôtel ou des centres construits spécialement pour les accueillir. C'est par exemple le cas dans le Territoire du Nord, où cette supervision coûte 2500 dollars (1700 CHF) par personne ou 5000 dollars (3400 CHF) par famille. En Australie-Occidentale, comme dans d'autres États, un centre de 1000 lits à l'aéroport de Jandakot est en cours de construction, mais il ouvrira ses portes en 2022.

Un dispositif national ?

Home Quarantine SA, ce système de surveillance particulièrement intrusif déployé depuis le 23 août en Australie-Méridionale – « South Australia » en anglais – et qui devrait s'étendre au reste du pays-continent, est présenté comme une alternative pour rendre ces quarantaines plus agréables pour les personnes concernées, mais aussi moins coûteuses. Une économie bilatérale, car les États diminueraient du même coup leurs frais de construction et la mobilisation de leurs policiers.

Les premiers testeurs de ce dispositif sont ceux qui reviennent en Australie-Méridionale depuis la Nouvelle-Galles du Sud ou de Victoria. Les autres personnes qui souhaitent ou doivent réaliser leur quarantaine en Australie-Méridionale sont obligées de prouver qu'elles ont un endroit dans lequel s'isoler pendant quatorze jours, mais aussi qu'elles sont complètement vaccinées. Toutes doivent bien évidemment procéder à l'installation de l'application Home Quarantine SA.

Sur son site, le gouvernement présente son système comme un outil apportant « une assistance et des ressources ». Il effectue des «enregistrements en direct multiples et aléatoires pour confirmer que vous êtes bien à l'adresse enregistrée», mais offre aussi des « tests personnalisés et un calendrier pour vous aider à planifier et à gérer votre quarantaine », ou encore des « contrôles quotidiens des symptômes ».

Pour le premier ministre d'Australie-Méridionale, Steven Marshall, cette opération est un test pour réduire la propagation de l'épidémie de Covid-19 et « une partie des coûts » engendrés par les quarantaines. « Une cinquantaine de personnes » sont actuellement inscrites, précisait-il le 23 août à ABC News, avant d'ajouter que les Australiens de cet État « devraient être fiers de diriger un

programme pilote national de quarantaine à domicile ». Si l'essai est concluant, il sera élargi dans « les prochaines semaines » aux voyageurs internationaux.

Une autre application similaire développée par une entreprise australienne, G2G Now, est utilisée par le gouvernement d'Australie-Occidentale pour surveiller les personnes en quarantaine sur son territoire. Celles-ci disposent d'une fenêtre de cinq minutes pour se prendre en photo. Pour l'heure, l'installation de celle-ci repose encore sur le volontariat, sauf pour les personnes qui voyagent depuis une zone « à haut risque. »

La goutte orwellienne

L'Australie est relativement épargnée par la crise sanitaire. Si Sydney, Melbourne et sa capitale, Canberra, font face à leur troisième vague, 34 cas ont été recensés dans le pays pour 100 000 personnes au cours des sept derniers jours. À titre de comparaison, sur la même période, Israël en a recensé 782, les États-Unis 355 et la Suisse 206. Pourtant, les mesures mises en place sont très restrictives.

Le pays n'a jamais rouvert ses frontières depuis leur fermeture en mars 2020, provoquant le blocage de plus de 35 000 de ses ressortissants à l'étranger et l'impossibilité de voyager pour ceux qui sont dans le pays – sauf dérogation exceptionnelle. Le déploiement de l'application de surveillance Home Quarantine SA est perçu comme la goutte orwellienne qui fait déborder le vase du supportable.

Le journaliste américain Conor Friedersdorf a notamment publié ce 2 septembre dans *The Atlanti*c un billet d'opinion au vitriol sur ce sujet. Il écrit :

> Si un pays interdit indéfiniment à ses propres citoyens de quitter ses frontières, bloque des dizaines de milliers de ses citoyens à l'étranger, impose des règles strictes sur les voyages intra-étatiques, interdit à ses propres citoyens de quitter leur domicile sauf s'ils ont une excuse officielle […] impose des masques même lorsque les gens sont à l'extérieur et respectent la distanciation sociale, déploie l'armée pour faire respecter ces règles, interdit les manifestations, arrête et inflige des amendes aux dissidents, ce pays est-il toujours une démocratie libérale ?

Le premier ministre australien, Scott Morrison, a déclaré il y a quelques semaines que son pays rouvrirait ses frontières dès que 80 % de la population adulte serait entièrement vaccinée contre le coronavirus. Aujourd'hui, moins de 40 % de la population l'est.

Source
The Conversation
Yann Bruna
8 novembre 2022

10. Géolocalisation des enfants : une nouvelle forme de surveillance parentale

Parmi les stratégies des parents pour surveiller les activités de leurs enfants, la géolocalisation est une pratique à la fois singulière et de plus en plus courante. Singulière, dans la mesure où la demande parentale de transparence vis-à-vis des usages numériques de leurs adolescents s'arrête le plus souvent aux frontières du domicile, alors que la géolocalisation dépasse nettement ce cadre. Courante aussi, car de nombreuses applications mobiles sont aujourd'hui focalisées sur le suivi géographique des jeunes au sein du cercle familial (Find My Kids, Google Family Link, Apple FindMy, etc.)

Comment les jeunes vivent-ils le fait d'être localisés et quelles sont les conséquences potentielles de ce traçage sur leur autonomisation ? Comment le dispositif technique s'inscrit-il dans l'exercice de la parentalité ? Enfin, le recours à la géolocalisation dans le cercle familial joue-t-il un rôle sur la communication ou encore la relation de confiance entre parents et enfants ?

Ce sont des questions que nous avons explorées à travers un travail de recherche constitué d'une série d'entretiens individuels menés auprès de parents qui ont déclaré géolocaliser leur(s) enfant(s) d'une part, et d'adolescents qui ont déclaré être géolocalisés d'autre part (qui sont, pour certains, les enfants des parents interrogés). Retour sur les principaux résultats.

Un enjeu sécuritaire

Selon les parents de notre enquête, le recours à la géolocalisation ne résulterait pas d'un excès de curiosité ni même d'une volonté d'envahir la vie privée des enfants. Cela traduirait plutôt une volonté de bienveillance face à un environnement extérieur propice au danger ou, a minima, à

l'incertitude.

Précisons que les parents interrogés se situent exclusivement dans des zones urbaines, une donnée importante ici puisque leurs témoignages mettent en avant les risques inhérents à la ville : « quand je vois ce qu'il se passe dans certains quartiers, je suis très content quand ma fille part et qu'elle m'appelle », explique Virginie, 38 ans, professeure des écoles. Commercial de 46 ans, Stéphane ajoute : « quand vous voyez ce qu'il s'est passé à Nice, je me dis que pour ne pas vouloir savoir où se trouvent ses enfants, il faut être irresponsable ».

Si Virginie ne localise qu'occasionnellement sa fille et reste le plus souvent dans l'attente de son appel, Stéphane est plus tranché : parce que l'outil est désormais à disposition, ne pas y avoir recours engage, selon lui, la responsabilité parentale. Si l'information géographique ne garantit en rien la sécurité des enfants face à des aléas qui se produisent en temps réel, la vérification de leur emplacement servirait à colmater au moins en partie le réservoir de peurs des parents.

Le cas des quartiers jugés « sensibles » par les parents n'est pas sans rappeler les travaux de Clément Rivière sur l'identification et la gradation d'espaces perçus comme « protégés » en dehors du chez-soi, sous-entendant que d'autres ne le sont définitivement pas.

L'usage de la géolocalisation ne permettrait pas seulement de vérifier la position de l'enfant, mais aussi de le situer spatialement – et donc socialement – par rapport à un ensemble de lieux identifiés comme plus ou moins sécurisants en ville.

Répondre à des incertitudes

Pour d'autres parents interrogés, le suivi de la position géographique ne s'effectue que si l'enfant ne répond pas à un appel ou à une sollicitation. Cette modalité de surveillance n'est pas systématique, elle s'apparente à un « dernier recours », lorsque l'exigence parentale d'être joignable ne se trouve pas comblée.

Mohamed, cadre dans le privé de 39 ans, montre qu'il s'autorégule dans son recours à l'outil, car il explique que géolocaliser son fils est « malsain », sauf dans une situation bien précise : « s'il n'est pas rentré à l'heure prévue, qu'il ne répond pas au téléphone, voilà… Ce sont des cas où l'on commence à paniquer ».

Alexandre, pâtissier de 54 ans, développe que c'est la conformité de la position géographique de l'enfant avec celle qui était attendue qui s'avère rassurante, car il vit avec « le doute de savoir si la personne va bien » et le besoin de savoir si « en fonction d'où elle (sa fille) est, c'est normal ou pas ».

Pour ces raisons, il « ne supporte pas » que sa fille contourne les limites qu'il impose via l'application et, si elle coupe son téléphone au cours de la journée, entend bien en discuter plus tard avec elle. La géolocalisation peut donc s'imposer comme la recherche d'une réponse à une non-réponse, lorsque l'enfant n'est pas disponible.

Des réceptions plurielles

À la condition que celle-ci soit perçue comme nécessaire, la géolocalisation semble a priori plutôt bien acceptée par certains adolescents de notre enquête. Le discours sécuritaire parental semble avoir été intériorisé par exemple par Mélanie, 13 ans, qui explique que lorsqu'elle regarde les informations, « il se passe toujours des trucs aberrants », avant d'ajouter : « au moins s'il y a un souci, tes parents savent où tu es ».

Elise, 14 ans, s'est également rendu compte de l'intérêt de la géolocalisation à la suite d'une expérience négative lors d'une sortie en ville : « Je marchais, je sens que quelqu'un me prend par l'épaule et ma mère, plus tard, m'a expliqué que c'était un pervers. Et c'est pour ça que des fois elle met la localisation, c'est vraiment rassurant pour moi ».

Cependant, de façon générale, les adolescents de notre échantillon ont majoritairement un point de vue critique sur l'utilisation d'applications de contrôle parental. Lorsque nous leur demandons si quelque chose va trop loin dans les possibilités offertes par ces applications, leurs réponses convergent presque unanimement vers la restriction du temps passé sur les réseaux sociaux et la géolocalisation.

Cette dernière « fait partie des limites » (Dylan, 16 ans) puisque « chacun doit avoir une vie privée, surtout à un certain âge » (Florian, 17 ans). Pour Julie, 16 ans, le recours à cette technologie est assimilé à une défaillance dans l'exercice de la parentalité : « Je trouve que quand tu es parent, c'est un échec de surveiller tes enfants comme ça pour voir s'ils te mentent ou pas sur ce qu'ils font et où ils vont ».

Paroles versus données objectives

Dans le cas d'une non-conformité entre une localisation attendue et une localisation vérifiée, le discours des adolescents interrogés met aussi en avant la violence d'un dispositif de traçage qui ne laisse que peu de place à la contextualisation, et encore moins à la dissimulation.

Contrairement aux messages ou aux photographies, qui laissent une certaine marge d'interprétation, il semble plus difficile pour les jeunes interrogés de développer un discours pour justifier leur position géographique lorsque celle-ci n'est pas conforme à ce qui était attendu.

Si plusieurs des adolescents de notre enquête ont déjà vécu cette situation, nous retiendrons le témoignage de Xavier, 15 ans, qui ne savait pas qu'il était géolocalisé par son père quand il a manqué un cours de rattrapage pour aller retrouver un ami et jouer à des jeux vidéo. À son retour au domicile familial, il a fait l'expérience d'une technologie qui ne lui a guère laissé la possibilité de discuter avec ses parents :

> « (Mon père) m'a demandé si j'étais bien allé au soutien, j'ai menti (…). Il m'a montré la tablette et tu ne peux rien dire contre ça, tu as tout de marqué, là où tu étais, à quelle heure… »

Ainsi présentée à l'écran, la donnée objective laisse bien moins de place à la subjectivité des échanges et des discours. Pour Xavier, la tablette – qui affiche l'historique de ses déplacements – fait figure de preuve et s'impose face à toutes formes d'argumentation. Cette métaphore judiciaire met en avant la confiance accordée à la fiabilité des dispositifs numériques et à la donnée de géolocalisation en particulier : l'outil, lui, ne ment pas, et la donnée affichée prévaut sur la parole de l'adolescent.

Une confiance mise à l'épreuve

Dans ce contexte, le recours à la géolocalisation n'est pas sans conséquence dans les relations intrafamiliales. Par exemple, depuis qu'il a appris qu'il était géolocalisé, Xavier déclare que cet épisode a profondément bouleversé la confiance réciproque entre son père et lui. La rupture s'est effectuée de part et d'autre, car en apportant la preuve que l'adolescent mentait sur ses déplacements, le dispositif a selon lui mis en avant que son père doutait de lui : « si tu n'as pas un doute, tu ne vas pas chercher à installer un truc comme ça ».

Julie et Océane ressentent également « un manque de confiance ». Les jeunes filles insistent sur leur âge (15 et 16 ans respectivement), ce qui pourrait montrer qu'elles perçoivent dans cette surveillance parentale une certaine infantilisation.

Cette tension dans le recours ou non à l'outil peut se situer du côté des parents, notamment dans le cas d'une garde partagée : « J'en ai déjà parlé plusieurs fois avec mon ex-femme, elle a sa façon de faire avec les filles, moi j'ai la mienne, on n'a pas la même vision dans ce domaine », explique Mohamed. Le père de famille argumente sur la source de ce désaccord : « La confiance, c'est important, si on flique ses enfants, il n'y a pas de confiance. Et s'il n'y a pas de confiance entre un père et son fils, ce n'est vraiment pas bon ». La géolocalisation des proches met donc en lumière une pluralité d'asymétries entre les individus, selon qu'ils soient à l'origine du traçage ou qu'ils en fassent l'objet.

La possibilité de surveiller sans être surveillé, la difficulté de se déconnecter sans que le surveillant n'en soit notifié ou encore la prévalence de la donnée sur le discours du surveillé jouent un rôle dans l'amplification du déséquilibre entre des parents de mieux en mieux informés, et leurs enfants qui doivent composer avec des vérifications de présence et d'activité de plus en plus nombreuses.

Alors que l'encadrement des activités numériques des jeunes restait spatialement limité au seul domicile (consultation de l'historique web, vérification a posteriori des photos prises, des applications installées, etc.), le suivi géographique questionne directement l'apprentissage des mobilités juvéniles non accompagnées et pourrait donc apparaître comme une entrave à l'autonomie des adolescents, en plus d'être l'objet de tensions dans les relations parentales et filiales.