GÉOLOCALISATION : LA BANALISATION DE LA SURVEILLANCE

Notre vie numérique est parsemée d'actions, de traces invisibles à l'œil nu que nous laissons derrière nous lors de notre passage sur le net. Ces empreintes sont enregistrées, collectées sur des serveurs par des firmes dans une visée de marketing. Parmi les données, on trouve celle de la géolocalisation. Où que l'on se trouve sur le globe, on peut aujourd'hui identifier notre position. Serions-nous traqués ?

Wifi, balises, relais téléphoniques, Bluetooth, carte SIM :

Souriez, vous êtes tracés !

Vous vous rendez régulièrement cheWz votre petit ami ? Vous êtes tracés. Vous allez souvent à la messe ? Encore tracés. Vous fréquentez les bars gays ? Toujours tracés. Vous passez régulièrement devant tel type de magasin de fringues ? Encore et toujours tracés. Vous allez me dire qu'il suffit de désactiver le GPS de votre téléphone pour être tranquille… sauf que non ! Même si vous désactivez cette option, vous êtes toujours localisable. Comment est-ce possible ?

Il existe plusieurs façons d'identifier votre position :

- Par **GPS**, c'est-à-dire via les satellites.
- Par le **wifi**.
- Par les **relais téléphoniques ou Données mobiles** (2G, 3G, 4G et bientôt 5G !).
- Via le **Bluetooth** et l'installation d'une application sur votre smartphone. En Belgique, la banque KBC utilise ce système via son application mobile.
- Mais aussi via les ***beacons***, balises disposées notamment dans les commerces aux Etats-Unis mais aussi en France et bientôt chez nous. Ce n'est pas de la géolocalisation proprement dite dans le sens où c'est plutôt un système qui vous envoie des messages lorsque vous vous trouvez à proximité. Si on ferme la géolocalisation, les beacons ne sont pas pour autant désactivés.
- La **Carte SIM** de votre téléphone mobile peut également enregistrer des données de localisation. Proximus propose à des sociétés diverses, des données de localisation que l'entreprise collecte sur les cartes SIM des appareils mobiles de ses clients. Ces données sont anonymisées.

Elliot Alderson, vous connaissez ? C'est ce jeune ingénieur en sécurité informatique qui est au centre de la série américaine Mr Robot, que je vous recommande au passage. Ce cyber-justicier anti-système souffrant de troubles de l'anxiété et de paranoïa recouvre sa webcam d'un scotch, se balade dans la rue avec un capuchon sur la tête pour ne pas être identifié par les caméras de surveillance, surfe sur le darknet et utilise tous les subterfuges pour être invisible... Et dans la vraie vie, ça marche comment ?

Toute une série d'applications ont basé leur modèle économique sur la géolocalisation. Par exemple **Tinder**, une appli qui permet d'identifier des personnes célibataires dans les environs d'où vous vous trouvez, mais aussi **Uber** ou **Google Map**. Sans géolocalisation, pas de business pour ces applis. Les systèmes d'exploitation comme Android, qui appartient à Google (l'un des leaders en matière de commercialisation des données personnelles), collectent également des données de géolocalisation.

Les panneaux publicitaires vous épient

Aujourd'hui, il est possible pour les annonceurs d'adapter la publicité qui s'affiche sur votre téléphone mobile **lorsque vous passez devant un panneau publicitaire** ; il suffit pour cela que vous ayez accepté le message de localisation. C'est bien connu, beaucoup de gens qui se baladent en rue aujourd'hui, ont souvent les yeux rivés sur leur smartphone et ne sont pas attentifs à leur environnement. En 2019, on estime que près d'une publicité sur deux envoyée sur nos mobiles sera géolocalisée.(1)

1. Géolocalisation : tous traqués ? Sophie Roland, Vincent Kelner et Dominique Morteau, Envoyé spécial, 12 février 2015.

Une intrusion permanente

Après tout, la plupart des gens aujourd'hui, en partageant un selfie par exemple, indiquent l'endroit où il a été pris, dans quel restaurant ils sont en train de manger ou de boire un verre… Beaucoup partagent leurs bons plans, les hôtels qu'ils fréquentent… Dans ce cas, vous choisissez vous-même d'être localisables, c'est votre propre choix. Mais lorsqu'on vous l'impose, c'est une autre histoire. Et vous n'imaginez pas tout ce que Google récolte sur vous sans votre autorisation, ou en tout cas sans que vous ne le sachiez parce que vous n'avez pas lu les conditions générales. Les firmes qui collectent vos données savent à quelle heure vous allez dormir grâce à l'heure à laquelle vous n'êtes plus actif sur les réseaux sociaux ou sur internet… Elles connaissent vos habitudes : à quelle heure vous sortez de chez vous le matin, si vous déposez vos enfants dans telle école, si vous vous rendez régulièrement dans tel hôtel, où vous allez faire vos courses…

Du coup, même si vous essayez de soigner votre identité numérique, que vous contrôlez les photos de vous que vous postez, que vous ne mentionnez pas les restos où vous vous rendez, les algorithmes des grandes sociétés qui récoltent les données, eux, seront capables de mettre à jour votre vraie identité, votre identité physique, celle que vous voulez cacher derrière vos selfies sur les réseaux sociaux.

De plus, les **objets connectés** qui commencent à faire partie de notre quotidien présentent d'énormes failles. Par exemple, les montres qui enregistrent notre rythme cardiaque et nos trajets, ou les poupées connectées censées apporter une sécurité à vos enfants, sont facilement « piratables ». Il en existe tout de même qui sont plus sécurisés que d'autres ; renseignez-vous bien lors de l'achat de l'un de ces nouveaux joujoux !

Les données de géolocalisation sont encore plus intrusives que les autres types de données que l'on collecte sur nous.
En 2014, la CNIL (Commission nationale informatique et libertés)[1] a publié une étude réalisée pendant trois mois sur les deux cents applications les plus utilisées par les Français. Celle-ci a révélé que 30% des applis ont eu accès à la localisation. **L'appli météo** ou **l'appli Playstore** installées par défaut sous Android, ont chacune géolocalisé les smartphones en test 1,5 million de fois pendant 3 mois à savoir 10 accès par minute ! Par contre, sur IOS, le système d'exploitation mobile développé par **Apple,** moins de données sont mesurées que sous Android, système d'exploitation mobile développé par Google.

A quelles informations ces applications ont-elles accès ? Au nom de l'opérateur, au numéro de série du téléphone, au numéro de téléphone, aux identifiants de la carte SIM, à la liste des points d'accès wifi : ceux-ci sont cartographiés dans le monde. En ayant accès à la liste des wifi déjà utilisés par votre téléphone, on va pouvoir déterminer les lieux où vous vous êtes rendus.

Le géomarketing a de beaux jours devant lui. Il permet d'ajuster un message en fonction d'un territoire donné. Par exemple, en analysant les données du site internet qu'une société gère, elle peut se rendre compte qu'elle a moins de visites de personnes qui se trouvent dans la province du Luxembourg. Elle peut alors prévoir une campagne de communication pour attirer ces personnes-là, par exemple, en leur proposant une offre d'abonnement alléchante. Vous l'aurez compris, si vous vous trouvez à Bruxelles, vous n'aurez pas le même avantage.
Vous avez sans doute aussi remarqué que depuis quelque temps, les sites ou **applis de médias en ligne** vous proposent de vous localiser. Cela leur permet de vendre cette donnée à des publicitaires qui pourront ainsi adapter l'offre à votre localité.

Du marketing au flicage

Qu'un inconnu connaisse vos trajets quotidiens ou vos comportements d'achats n'a peut-être pas beaucoup d'importance pour vous. Mais c'est sans compter sur l'énorme pouvoir qu'ont les sociétés qui détiennent toutes ces données sur nous : que diriez-vous de devoir utiliser une appli qui enregistre votre comportement de conduite en temps réel ? En échange, votre assureur vous donnerait une ristourne si vous obtenez un bon score ! Certaines entreprises utilisent également cette technologie pour surveiller leurs salariés : suivre leur temps de travail, les livraisons… Bien qu'un cadre juridique existe, c'est la question de la banalisation de la surveillance qui est en jeu.
Entre sécurité et surveillance, la distance est ténue. Au nom de la sécurité, on justifie l'usage de technologies qui nous épient. La surveillance est brandie comme un moindre mal, une évolution naturelle et l'on doit faire confiance aux autorités qui ont accès à notre vie privée. Comment faire aujourd'hui si l'on ne souhaite pas être tracé ? Etre attentif au type d'applis que l'on télécharge ? Désactiver le GPS de son téléphone et de son appareil photo ? Couper le wifi, les données mobiles et le Bluetooth ? Est-ce pour autant envisageable ? En théorie sans doute. Qui va penser à chaque fois qu'il aura terminé d'utiliser son smartphone, à réaliser ces actions ?

Au-delà de la prise de conscience des individus, de la nécessaire information, de l'échange utile de trucs et astuces, c'est le modèle

1. La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

qu'il faut questionner : est-ce normal que Google Maps soit l'application de référence utilisée par d'autres applis ? N'y a-t-il pas là un problème de monopole et donc de concentration de données dans les mains de quelques géants du Net ? Des alternatives existent mais elles ne sont pas suffisamment connues (Startpage, Openstreetmap…) et manquent de moyens pour se perfectionner et proposer des outils aussi faciles à utiliser que l'offre Google. Une solution serait de demander aux autorités compétentes de promouvoir et investir dans ce type de projet.

Est-ce normal que certains pays européens utilisent les données, notamment de géolocalisation, des migrants pour vérifier leurs dires ? N'est-ce pas là une grave atteinte aux droits de l'homme ? N'est-ce pas là aussi le signal d'une dérive ? Qu'est-ce qui nous garantit que nos faits et gestes resteront consignés à un seul endroit ou seront utilisés uniquement à des fins clairement identifiées ? Et plus simplement, avons-nous, sans nous en rendre compte, abandonné à jamais notre droit à l'anonymat, le plaisir de nous fondre dans la masse, de nous perdre au détour d'une ruelle sans pour autant que des inconnus parfois même à l'autre bout du monde ne soient au courant ? Avons-nous délaissé une fois pour toute la sensation enivrante que peut procurer la liberté de mouvement ?

Claudia Benedetto

Trahis par le Bluetooth…

Certains centres commerciaux en France et maintenant en Belgique vous proposent une appli qui vous renseigne sur les promotions et qui vous guide vers le produit que vous désirez. Attendez-vous à recevoir une flopée de notifications au moindre mouvement, dès que vous passez devant les magasins mais aussi dans leurs enceintes. Vous n'êtes que de passage dans le rayon des sous-vêtements, qu'importe ! Votre téléphone sonne pour vous rappeler qu'il y a une promo à saisir sans tarder. Vous ne comptiez pas acheter de brosse à dents aujourd'hui ? Pas grave, votre smartphone est toujours là pour vous rappeler qu'une offre incroyable est à portée de main ! Comment cela est-il possible ? Il suffit de vous géolocaliser sur l'appli du centre commercial, d'activer votre Bluetooth et le tour est joué : une petite boite noire installée dans les magasins vous renvoie un signal quand vous passez à proximité. C'est une aubaine pour les commerçants qui leur permet d'analyser vos goûts, identifier le rayon le moins attractif et trouver une stratégie pour vous y attirer quand même. En Belgique, cette technologie n'est pas encore bien implantée, mais à Namur et à Bruxelles, des balises ont été installées sur les devantures de certains magasins : l'application qui permet de faire fonctionner le dispositif a déjà été téléchargée par plus de 1.000 personnes.

Trois lieux suffisent pour connaître vos amis !

Vous localiser permet d'avoir accès à toute une série d'informations vous concernant : « *Pour identifier de manière unique une personne, il suffit d'avoir accès à trois points de géolocalisation. Parce que personne n'a le même triplé d'informations : personne n'a le même travail que vous ; le même domicile que vous, le même loisir que vous* » explique Stéphane Petitcolas, ingénieur expert à la CNIL, à l'occasion des Assises du Géomarketing 2015 [1].

Tout cela est possible par exemple en analysant la fréquence à laquelle on vous localise à un endroit précis. Mais ce n'est pas tout ! On peut aussi savoir qui sont vos vrais amis dans la vraie vie ! Pour ce faire, les analystes qui réceptionneront vos données analyseront le nombre de fois que vous vous trouvez au même endroit qu'un autre appareil, si cela se reproduit quatre fois, on pourra en déduire que vous êtes avec un proche.

1. Stéphane Petitcolas présente la protection des données personnelles sur l'utilisation de la géolocalisation par les smartphones à l'occasion des Assises du Géomarketing 2015.