L'Heure du Peuple
Pour la 6e République
Journal insoumis

À fond Coronavirus, cybersurveillance
1 avril 2020
Jill Royer

Coronavirus et cybersurveillance

Depuis le mardi 24 mars, le nouveau conseil scientifique réuni par l'Élysée réfléchit à la mise en place de dispositifs de pistages géographiques des citoyens, pour combattre l'épidémie de Coronavirus. Nicole Belloubet a annoncé ne pas y être opposée, mais qu'il fallait encore réfléchir au sujet. Réfléchissons alors : de quoi parle-t-on exactement ?

Quels sont les données existantes ?

Il existe deux moyens de géolocaliser quelqu'un par son téléphone. Premièrement la plupart des téléphones intelligents disposent aujourd'hui d'un GPS. Le GPS utilise ses propres ondes radios, il fonctionne donc dès que le téléphone est allumé, même sans accès au réseau mobile. Un GPS est comme une boussole : le simple fait d'en utiliser un ne transmet pas la position de l'appareil à qui que ce soit. Cependant, les téléphones équipés de GPS enregistrent cette position et la transmettent aux nombreuses applications installées qui souhaitent l'utiliser. Google Maps, Tinder, Facebook, TripAdvisor demandent toutes à votre téléphone de lui transmettre les données du GPS.

Deuxièmement, il est possible de géolocaliser un téléphone par la manière dont il se connecte au réseau. Le réseau de téléphonie mobile est constitué d'un maillage d'antennes-relais sur tout le territoire. Chacune a un rayon de couverture allant de quelques centaines de mètre à plusieurs kilomètres, selon la densité de population de la zone où elle est installée. Lorsqu'on se déplace, notre téléphone passe d'une antenne à une autre. Les opérateurs téléphoniques peuvent donc savoir en permanence à quelle antenne sont connectés leurs abonnés. Par ce moyen, il n'y a donc pas besoin de GPS pour connaître la position de quelqu'un, il suffit qu'il soit connecté au réseau. Par contre, un téléphone en mode hors-ligne ne peut pas être géolocalisé. Ses données sont aussi moins précises : alors que le GPS donne une position à quelques mètres près, la géolocalisation par l'antenne relais dépend de l'étendue de la zone de couverture de celle-ci.

Qui a accès à ces données ?

Ces données de géolocalisation existent donc déjà. En France, les télécoms étant historiquement bien plus régulés que les GAFAMs, c'est dans un premier temps aux données téléphoniques que l'État s'intéresse. La question posée actuellement est surtout celle de leur compilation, leur traitement, et qui y a accès. De nombreux usages pré-existent déjà à la crise actuelle.

Souvent, les données sont "agrégées", c'est à dire que les données individuelles sont additionnées et compilées pour en faire des statistiques. Les statistiques nationales du trafic de téléphonie mobile (la quantité d'appel et de SMS échangés) sont même des données diffusées publiquement chaque trimestre. Les données agrégées au niveau local peuvent servir en interne aux opérateurs téléphoniques : elles leur permettent de dimensionner le réseau en fonction de son usage réel.

C'est à ce type de données agrégées que la Commission Européenne a demandé l'accès aux opérateurs à la mi-mars. Orange va ainsi transmettre des données agrégées à partir de ses 35 millions d'abonnés. En début de semaine, l'opérateur a aussi collaboré avec l'INSEE. Ils ont ainsi mis en lumière que 17 % des habitants d'Île-de-France avaient quitté la région pour se réfugier ailleurs en France depuis le début du confinement.

Données anonymisées : le risque existe quand même

Bien qu'Orange et la Commission aient annoncé que ces statistiques seraient anonymisées et agrégées, il faut demander à contrôler démocratiquement la manière dont cela sera fait. En effet, l'anonymisation de données personnelles n'est pas une tâche simple : il ne suffit pas de remplacer le nom de la personne dans un fichier par un numéro anonyme. Les données de géolocalisation sont extrêmement faciles à "désanonymiser", c'est à dire qu'on peut facilement retrouver l'identité d'une personne, quand bien même son nom est absent des données : il suffit de savoir où elle habite et où elle travaille, pour retrouver, à partir de sa position, la ligne de données qui la concerne et ainsi tous ses autres déplacements. Qu'on accepte ou non que de telles statistiques sur les données des opérateurs aient lieu, il faut donc au moins demander à ce que soient rendues publiques les méthodes d'anonymisation et qu'un contrôle démocratique soit exercé sur celles-ci.

Le pistage individuel : un atteinte à la vie privée

Une étape beaucoup plus dangereuse serait d'utiliser ces moyens de géolocalisation pour faire de la surveillance individuelle. La loi de renseignement de 2015 permet déjà à l'État d'utiliser des dispositifs de géolocalisation pour un grand nombre de délits et crimes, ainsi que pour des intérêts nationaux. En particulier, cette loi autorise l'administration à demander la transmission de données de géolocalisation personnelles aux opérateurs téléphoniques, sans même le contrôle d'un juge. Elle l'autoriserait donc à utiliser des données personnelles pour lutter contre le coronavirus.

La tentation est grande : en Corée du Sud, en Chine ou en Israël, la géolocalisation est utilisée pour lutter contre le virus. Une fois que quelqu'un est dépisté, elle sert à identifier les personnes qui sont rentrées en contact avec elle et les en avertir, afin qu'elles se fassent dépister elles aussi. De manière plus coercitive, elle peut servir aussi à vérifier qu'un individu respecte bien une mesure de confinement obligatoire.

En Israël, les services de renseignements ont ainsi directement accès aux données des opérateurs téléphoniques.

En Corée du Sud, cela va même plus loin. Afin d'obtenir des données encore plus précise, certaines personnes, notamment celles qui rentrent de l'étranger, sont obligées d'installer une application gouvernementale, qui utilise les données GPS du smartphone pour les transmettre directement aux autorités.

Ces politiques n'ont cependant aucune efficacité prise isolément : elles ne permettent d'endiguer la propagation de virus que lorsqu'elles sont associées à des politiques de dépistage massif. En France, ces dépistages n'existent pour l'instant même pas, elles n'auraient donc aucun sens.

Mais même associé à un dépistage, c'est au peuple de décider s'il est prêt à sacrifier son droit à la vie privée. Or, les avantages offerts par de telles mesures sont bien maigres : il est possible d'identifier la

plus grande part des contacts qu'a eu une personne dépistée, et de les en informer, sans forcément automatiser cette tâche par la géolocalisation.

Les désavantages sont par contre énormes : si le simple prétexte de la maladie pouvait servir à accéder aux données personnelles d'un citoyen, on imagine la quantité de personnes que la police pourrait surveiller, sans contrôle judiciaire, et les dangers de cet outil entre les mains d'un gouvernement déjà trop autoritaire.

Les périodes de crises servent souvent à mettre en place des mesures, présentées comme exceptionnelles, qui entrent ensuite dans le droit commun. Ce fut le cas avec l'état d'urgence contre le terrorisme. Il ne faut pas que ce soit le cas avec la cybersurveillance des citoyens et le coronavirus.

Jill Royer

Image par MasterTux de Pixabay