# Surveillance de l'épidémie: la Cnil met en garde le gouvernement

PAR GÉRALDINE DELACROIX ET JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE JEUDI 26 MARS 2020

Alors qu'un projet « d'identification des personnes ayant été au contact de personnes infectées » se met en place, l'autorité chargée de la protection des données personnelles demande à l'État *« de privilégier le traitement de données anonymisées »*.

Alors que l'Élysée vient de lancer une réflexion sur l'utilisation des données de géolocalisation des téléphones mobiles afin de lutter contre l'épidémie de Covid-19, la Commission nationale de l'informatique et des libertés (Cnil) appelle les autorités, dans une série de recommandations transmises mercredi 25 mars, dont Mediapart a pu prendre connaissance, à respecter certains principes afin de préserver les libertés individuelles.

Les recommandations de la Cnil sont formulées au lendemain de l'annonce, par la présidence de la République, de la mise en place d'un Comité analyse recherche et expertise (CARE) chargé, notamment, *« de conseiller le gouvernement pour ce qui concerne les programmes et la doctrine relatifs aux traitements, aux tests et aux pratiques de "backtracking" qui permettent d'identifier les personnes en contact avec celles infectées par le virus du Covid-19 »*. Le comité *« accompagnera par ailleurs la réflexion des autorités sur la doctrine et la capacité à réaliser des tests ainsi que sur l'opportunité de la mise en place d'une stratégie numérique d'identification des personnes ayant été au contact de personnes infectées »*, poursuivait le communiqué.

Aucun détail n'a été donné sur les options techniques retenues par les autorités. *«Plusieurs scénarios seraient envisageables, et les impacts sur les droits et libertés fondamentaux des personnes seraient fonction du type de traitement réalisé sur les données de localisation*, rappelle tout d'abord la Cnil. *Le cadre juridique actuel, en particulier le RGPD et la directive ePrivacy (applicable au recueil de données de localisation dans le cadre de communications électroniques), permet, selon certaines modalités, de traiter de telles données notamment de manière anonymisée (suffisamment agrégée) ou avec le consentement des personnes. Ce même cadre juridique permet aux États d'aller plus loin et de déroger, par la loi, à cette exigence d'anonymisation ou de consentement, sous certaines conditions. »*

*« Pour limiter l'impact sur les personnes »*, la Cnil demande à l'État *« de privilégier le traitement de données anonymisées et non de données individuelles, lorsque cela permet de satisfaire l'objectif »*. Dans les cas où un suivi individuel serait nécessaire, *« ce suivi devrait reposer sur une démarche volontaire de la personne concernée »* sur le modèle des *« applications de "contact tracing" existantes »*.

*« Si la France souhaitait prévoir des modalités de suivi non anonymes plus poussées, le cas échéant sans le consentement préalable de l'ensemble des personnes concernées, une intervention législative s'imposerait*, poursuit la Cnil. *Il faudrait alors s'assurer que ces mesures législatives dérogatoires soient dûment justifiées et proportionnées (par exemple en termes de durée et de portée). »*

La commission appelle enfin les autorités à respecter *« dans tous les cas certains principes cardinaux »* devant guider leurs décisions : *« veiller à définir objectivement et précisément les objectifs poursuivis par tout dispositif de localisation »* et *« veiller à respecter les principes fondamentaux posés par la loi "Informatique et libertés" et les textes européens, qui sont des gages de confiance pour les personnes »*.

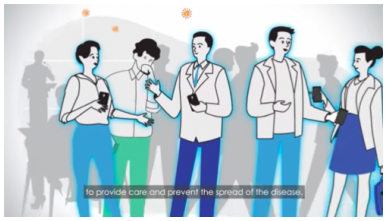


Image extraite de la vidéo de l'application développée par le gouvernement de Singapour.

Enfin, la Cnil *« se tient à la disposition des pouvoirs publics et des responsables de traitement pour accompagner les initiatives permettant de lutter contre la pandémie tout en protégeant la vie privée des personnes »*. Elle prévient que *« dès la fin de la crise, elle veillera à ce que les dispositifs exceptionnels*

*qui auraient été, le cas échéant, mis en œuvre soient sans conséquence pour les personnes concernées (destruction des données, etc.) et que ceux-ci ne soient pas pérennisés »*.

La violation du secret médical est un autre écueil auquel pourrait faire face tout projet de suivi individualisé des personnes. Interrogé sur ce point par Mediapart, le Conseil national de l'ordre des médecins nous a dit analyser *« cette information pour laquelle il n'a pas été sollicité. Il fera savoir, à la suite de cette analyse, ses exigences en matière de protection du secret médical »*.

L'idée d'utiliser les données personnelles des citoyens pour lutter contre la propagation de l'épidémie n'est pas nouvelle. De nombreux pays, tout d'abord en Asie et puis en Europe, ont très vite mis en place des dispositifs de surveillance parfois extrêmement liberticides, soit pour essayer de suivre la diffusion du virus, soit pour s'assurer que leurs citoyens respectent bien les mesures de confinement. En France, certains demandent que des mesures similaires soient prises, au nom de l'état d'urgence sanitaire.

Lors de l'examen par le Sénat de la loi instituant cet état d'urgence, les élus LR Bruno Retailleau et Patrick Chaize avaient ainsi déposé **un amendement**, rejeté par le gouvernement, autorisant pour une durée de six mois *« toute mesure visant à permettre la collecte et le traitement de données de santé et de localisation »*. Cet amendement était motivé par le fait de *« faciliter les procédures imposées aux opérateurs dans la collecte et le traitement des données de santé et de localisation »*.

Le lendemain, le PDG d'Orange, Stéphane Richard, annonçait **dans *Le Figaro*** que le groupe de télécommunication travaillait déjà avec l'Institut national de la santé et de la recherche médicale (Inserm) *« pour voir comment les données peuvent être utiles pour gérer la propagation de l'épidémie »*. Le but de ce partenariat, expliquait-il, est d'utiliser les données de géolocalisation anonymisées afin *« de permettre aux épidémiologistes de modéliser la propagation de la maladie »*.

Une utilisation en théorie contraire au Règlement général sur la protection des données personnelles (RGPD). *« Cela demanderait des ajustements réglementaires et un accord de la Cnil*, reconnaissait Stéphane Richard. *Ainsi, il faudrait pouvoir garder des données sur une durée de temps longue, or actuellement nous devons les supprimer au bout d'un an, nous voudrions les garder deux ans. »*

*« Les données pourraient aussi être utilisées pour mesurer l'efficacité des mesures de confinement, comme en Italie*, ajoutait encore Stéphane Richard. *Je le répète, nous parlons de données anonymisées et agrégées. Leur utilisation est indispensable pour mesurer le confinement et pour ajuster les dispositions en fonction des comportements. Il ne s'agit pas de traquer les gens individuellement. Il faut au moins savoir si les gens respectent les périmètres de confinement, ou s'ils se déplacent, sans pour autant savoir qui va où. »*

Lundi 23 mars, **le site Politico** révélait que Thierry Breton, le commissaire européen au marché intérieur, avait organisé une réunion téléphonique avec les dirigeants des principaux opérateurs européens, dont Orange et Deutsche Telekom, afin d'envisager avec eux un programme de transmissions des données de géolocalisation de leurs utilisateurs. *« Nous sélectionnerons un grand opérateur par pays »*, a précisé Thierry Breton à Politico. *« Nous voulons être très rapides et suivre ça sur une base quotidienne. »* Interrogée par Mediapart, la Commission européenne précise que la discussion porte sur *« l'utilisation de données agrégées et anonymisées »* qui permettront d'étudier *« l'impact des mesures de confinement »* sans *« suivre des utilisateurs individuels »*. Elle se dit *« en contact étroit avec le superviseur européen pour la protection des données »*.

Jusqu'à présent, aucune information n'a filtré sur l'usage que le gouvernement français envisagerait de faire de ces données. Une première possibilité serait d'utiliser les données de géolocalisation pour tenter de suivre les déplacements des usagers et ainsi que la propagation de la maladie. Mais cette solution pose

plusieurs problèmes, notamment techniques. Sans compter le repérage initial des personnes touchées par le virus et potentiellement contaminantes.

Techniquement, la précision des dispositifs de géolocalisation est en effet extrêmement variable et diminue très fortement dès que la personne entre dans un espace confiné, là où justement les risques de contamination sont les plus élevés. Ainsi, si la personne suivie entre dans un supermarché ou dans le métro, il est impossible de savoir dans quel rayon elle s'est baladée ni dans quelle rame elle est montée, et donc de savoir qui se trouvait à quelques mètres d'elle. Si le but était par exemple de tester ou de mettre en quarantaine les personnes potentiellement contaminées, c'est toutes les personnes présentes dans le magasin ou dans la rame qu'il faudrait viser.

L'autre utilisation possible des données de géolocalisation consiste à les exploiter de différentes manières afin de s'assurer que les personnes respectent bien leurs mesures de confinement. Plusieurs pays ont déjà déployé des dispositifs de ce type diversement invasifs, allant de la simple mesure incitative à la mise en place de systèmes de surveillance particulièrement coercitifs et élaborés.

L'État ayant été le plus loin dans ce domaine est sans doute Taiwan, qui soumet ses citoyens à un contrôle numérique intensif de leurs déplacements, soutenu si nécessaire par les forces de l'ordre. **Le gouvernement et les opérateurs** ont ainsi mis en place un système qui surveille les signaux téléphoniques pour alerter la police et les autorités locales si les personnes en quarantaine à domicile s'éloignent de leur adresse ou éteignent leur téléphone. Selon le chef du département de la cybersécurité, *« l'objectif est d'empêcher les gens de courir partout et de propager l'infection »*. Les autorités contacteront ou rendront visite à ceux qui déclenchent une alerte dans les 15 minutes. Les fonctionnaires appellent également deux fois par jour pour s'assurer que les gens ne trichent pas en laissant leur téléphone à la maison ***(lire également l'article de notre correspondante)***.

Dans le même esprit, la Pologne a mis en place, depuis le 19 mars, une application réservée aux personnes placées en quarantaine (dont les numéros de téléphone sont collectés), et basée sur les données de géolocalisation et la reconnaissance faciale. La quarantaine est obligatoire pendant 14 jours pour les personnes qui arrivent de l'étranger, et pour celles qui ont été en contact avec des personnes touchées par le coronavirus. **L'application** doit servir à surveiller le respect de cette quarantaine.

Les personnes en quarantaine pourront recevoir un texto inopiné. Après quoi, elles auront 20 minutes pour envoyer un selfie. Les services de police vérifieront que la personne se trouve dans le périmètre fixé pour la quarantaine, et qu'il s'agit bien de la bonne personne, grâce à la photo. Faute de réponse, la police pourra se déplacer. Le non-respect de la quarantaine est puni d'une amende qui peut aller jusqu'à 5 000 zlotys (un peu plus de 1 000 euros).

Toujours dans le registre coercitif, Benjamin Netanyahou a pris en Israël une ***« mesure d'urgence »*** qui autorise le service de sécurité intérieure (Shin Bet) à collecter *« immédiatement »* des données sur les citoyens afin de lutter contre la propagation du virus. Des centaines de personnes ont ainsi eu la surprise de recevoir un texto du ministère de la santé, signalant qu'elles avaient pu être en contact avec une personne infectée, et leur ordonnant de se placer immédiatement en quarantaine pour 14 jours.

Les données sont par ailleurs utilisées de manière agrégée, pour comprendre la façon dont les populations se déplacent ou restent confinées. C'est par exemple le cas en Lombardie, dont le gouvernement a conclu un partenariat avec les opérateurs de téléphonie, explique le ***Corriere Della Sera***. Selon le vice-président de la région, Fabrizio Sala, qui dressait le 17 mars le bilan quotidien de la situation sanitaire, 40 % de la population, beaucoup trop selon lui, effectuait encore des déplacements de 300 à 500 mètres.

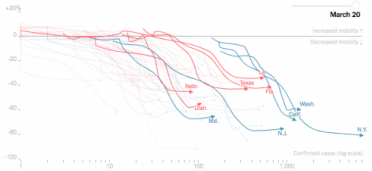
En Suisse, le quotidien ***Le Temps*** a révélé mercredi 25 mars que le gouvernement a demandé à l'opérateur de téléphone Swisscom d'identifier les zones comptant

au moins 20 cartes SIM dans un espace d'une superficie de 100 mètres sur 100. Le but, pour Berne, sera de déterminer si la population respecte l'interdiction de rassemblements de plus de cinq personnes dans l'espace public, à savoir les places publiques, les promenades et les parcs, comme le stipule l'article 7c, alinéa 1 de l'ordonnance 2 Covid-19.

En Grande-Bretagne, où **Google fait des offres de services**, c'est l'opérateur O2 qui a **donné au gouvernement** des données de géolocalisation agrégées, dans le but de visualiser la chute attendue des déplacements.

Aux États-Unis, Facebook et Google **discutent** avec le gouvernement fédéral pour trouver une utilisation aux données qu'elles collectent de toutes façons. *« Nous explorons les moyens par lesquels des informations de localisation anonymes agrégées pourraient aider* […]. *Un exemple pourrait être d'aider les autorités sanitaires à déterminer l'impact de la distanciation sociale »*, un peu comme les embouteillages dans Google Maps, a expliqué un porte-parole de Google Santé, soulignant qu'un tel partenariat *« n'impliquerait pas le partage de données sur la localisation, les déplacements ou les contacts d'un individu »*. Une *task force* créée par différentes entreprises et investisseurs a même présenté ses idées à la Maison Blanche.

Hors des circuits gouvernementaux, différentes sociétés se sont engouffrées dans le créneau de la prédiction. La compagnie Unacast, qui collecte et analyse les données GPS des téléphones, a lancé un **« tableau de bord de la distanciation sociale »**, comté par comté, sur le territoire des États-Unis. La société mesure la réduction des distances parcourues. Le *New York Times* a lui-même **produit des infographies** avec Descartes Labs, une compagnie spécialisée dans l'analyse des données géolocalisées.




Infographie réalisée à partir de données de géolocalisation et visualisant la chute des déplacements. © New York Times

IBM, de son côté, cherche avec **sa filiale météo** à mettre au point une carte de progression de l'épidémie, qui serait basée sur la récolte des informations sur les cas et les décès, comté par comté. L'idée est d'utiliser l'intelligence artificielle pour « checker » tous les quarts d'heure les informations publiées par les sites officiels locaux. Tandis que la société Kinsa, qui produit des thermomètres connectés, espère suivre la progression de l'épidémie **en temps réel**, forte de ses succès dans la détection de la propagation de la grippe.

À l'opposé de Taiwan, Singapour est jusqu'à présent le pays ayant développé la solution la moins intrusive et liberticide. Le gouvernement a en effet pris une autre option, celle d'une surveillance centrée sur l'utilisateur et plus respectueuse des libertés publiques. Les personnes sont fortement incitées à télécharger sur leur téléphone une application baptisée TraceTogether. Le but, ici, n'est pas de géolocaliser l'utilisateur mais d'utiliser la connexion Bluetooth de son appareil pour identifier les autres téléphones situés à proximité. Les données ne sont pas transmises mais stockées, de manière chiffrée, dans l'appareil. Si l'utilisateur apprend par la suite qu'il est porteur du virus, il doit alors contacter les autorités sanitaires et leur transmettre le fichier contenant les identifiants des téléphones des personnes qu'il a pu croiser. Celles-ci sont ensuite contactées pour être averties du risque de contamination.

Au-delà de différentes options technologiques, se pose également la question du régime juridique qui sera applicable à ces mesures d'exception qui violeront à coup sûr le droit commun. Les inquiétudes posées par les mesures exceptionnelles sont d'autant plus grandes

que la loi instaurant en France un « état d'urgence sanitaire » permet au premier ministre de prendre toute une série de dispositions d'exception. Ce texte a été adopté afin de remplacer le régime d'exception prévu par l'article L3131-1 du code de la santé publique. Celui-ci accordait des pouvoirs très larges au ministre de la santé mais prenait au moins la précaution de préciser que les pouvoirs publics *« sont tenus de préserver la confidentialité des données recueillies à l'égard des tiers »*. Une prudence qui n'a pas été reprise dans la loi.

*«* A priori, *il n'y a aucune raison que l'état d'urgence entraîne une suspension du cadre juridique existant. Le RGPD s'applique encore »*, estime Félix Tréguer, sociologue et membre de l'association de défense des libertés numériques La Quadrature du net. Celle-ci s'est inquiétée, **dans une analyse** publiée le 19 mars, des possibles dérives et a appelé le gouvernement à *« résister à toute fuite-en-avant sécuritaire »*. L'association rappelait par ailleurs que le droit existant permet déjà d'ordonner la collecte de données de géolocalisation, notamment la loi renseignement de 2015 qui offre aux autorités des pouvoirs de surveillance dans certains cas. *« À cadre juridique constant, la loi renseignement permet de prendre des mesures similaires*, affirme Félix Tréguer. *Une des sept finalités prévues par ce texte évoque la défense des intérêts économiques de la France. Vu les conséquences économiques de l'épidémie, nous sommes dans ce cas. Et ce texte autorise la géolocalisation. »*

*« Il faut aussi se demander si tout ça est efficace*, poursuit le sociologue. *Je pense par exemple que l'on a surestimé le dispositif de surveillance numérique chinois et son efficacité dans le ralentissement de l'épidémie. Certains chercheurs soulignent que ce n'est pas tant celui-ci que des mesures contraignantes physiques, comme le confinement forcé et l'installation de check-points dans les villes, qui ont eu un effet concret. Pour pouvoir juger de la proportionnalité de ces mesures, encore faudrait-il pouvoir prouver leur efficacité. »*

*« Il y a un buzz et une appétence pour aller vers ces approches technologiques qui ne sont pourtant qu'expérimentales sans que l'on se pose même la question de leur efficience*, pointe Félix Tréguer. *Cette période est l'occasion d'une grande campagne de marketing pour l'appareil techno-sécuritaire qui en profite pour faire des démonstrations de ses produits. Je pense notamment à l'usage de drones mis en scène par la préfecture de police à Paris ou à certaines start-up qui promettent de détecter les gens malades. Nous sommes dans une fuite en avant techno-sécuritaire. On peut se demander si ce solutionnisme technologique n'est pas un palliatif visant à masquer les vrais problèmes, à savoir le manque de moyens et de personnel et d'une manière générale la casse de l'hôpital public. »*

Félix Tréguer s'inquiète également des conséquences à long terme qu'aurait la mise en place de dispositifs de surveillance. *« Nous sommes dans un processus de sécurisation de cette crise qui a débuté par l'anaphase du président de la République lors de son intervention télévisée, "nous sommes en guerre", et qui se poursuivait encore aujourd'hui avec* ***le ministre de l'agriculture*** *qui a appelé les Français à "rejoindre la grande armée de l'agriculture française". On peut donc s'attendre à d'autres mesures d'exception. Le problème est que l'expérience montre que ce genre de période, ça laisse des traces dans les esprits et dans le droit. Il y a un risque de banalisation de certaines techniques de surveillance qui font aujourd'hui encore débat et de pérennisation de certaines mesures. »*

C'est exactement la même analyse que fait Edward Snowden, l'homme qui a révélé au monde la surveillance mise en place par les États-Unis après le 11-Septembre. *« La surveillance de masse ne fonctionne pas »*, affirme-t-il avec force dans un entretien réalisé pour le festival du film documentaire de Copenhague, annulé pour cause de coronavirus.

*« Qu'est-ce qui protège le mieux la santé publique ? »*, interroge le lanceur d'alerte. *« Est-ce que c'est la communauté, les médecins, les spécialistes, notre force collective »*, ou la surveillance ? *« Quand on perd un droit qui a pris si longtemps à être obtenu, dans*

*un moment de panique, là est la connexion avec le 11-Septembre. »« Dans une société libre, le virus est nocif, mais la destruction des droits est fatale »*, met en garde Edward Snowden depuis son exil moscovite.

## Boite noire

La réaction du Conseil national de l'ordre des médecins a été ajoutée jeudi matin.

**Directeur de la publication** : Edwy Plenel
**Direction éditoriale** : Carine Fouteau et Stéphane Alliès
**Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).**
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 24 864,88€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Laurent Mauduit, Edwy Plenel (Président), Sébastien Sassolas, Marie-Hélène Smiéjan, François Vitrani. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart, Société des salariés de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
**Courriel** : contact@mediapart.fr
**Téléphone** : + 33 (0) 1 44 68 99 08
**Télécopie** : + 33 (0) 1 44 68 01 90
**Propriétaire, éditeur, imprimeur :** la Société Editrice de Mediapart, Société par actions simplifiée au capital de 24 864,88€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.