Stopcovid un traçage dit « anonyme » !

Orange, Thales, Dassault Systèmes et quelques autres... font partie de l'équipe projet Stopcovid , projet qui consiste à mettre au point une application sur smartphone de traçage des individus, traçage que l'on nous certifie anonyme…
« …Les prises de position s'accumulent contre elle et son avenir semble chaque jour plus incertain.la CNIL a rendu un avis (6) à son sujet : elle exige que le gouvernement démontre l'utilité concrète de StopCovid, ce qu'aucune étude ou analyse ne soutient actuellement, mais s'est arrêtée en chemin en n'interdisant pas ce projet.

Ce projet a été mis en place avec l'idée que l'on pourrait combattre la diffusion du virus SARS-CoV-2 en retraçant les chaînes de transmission entre individus … »

« Mais à quoi sert une application de signalement si l'on ne peut pas dépister dans le même temps ? C'est à dire si on ne peut connaitre l'identité des individus ?
En pratique, une application anonyme n'aurait aucun intérêt : l'application doit envoyer à des personnes ciblées des alertes du type « vous avez été au contact de personnes malades, mettez-vous en quarantaine ». **Du moment que chaque alerte est envoyée à des personnes ciblées, le système n'est plus anonyme** : trivialement, il suffit qu'un tiers (un patron, un conjoint, etc.) puisse consulter votre téléphone pour constater que vous avez reçu une alerte. Des chercheurs·ses de l'INRIA ont produit une excellente liste de quinze scénarios (**5)** de ce type, démontrant à quel point il était simple de lever ce prétendu « anonymat ». **(1)**

« Comment ne pas s'interroger sur la possibilité d'utiliser StopCovid demain à des fins de surveillance plus autoritaire ? L'Etat ne peut être juge et parti. »

« Autre sujet de préoccupation particulièrement grave, l'utilisation des données. La révélation il y a quelques jours de l'intention du gouvernement d'autoriser la transmission de nos données de santé à l'américain Palantir dans le cadre de la lutte contre la pandémie ne facilite pas un climat de confiance.
Fournisseur du Pentagone, de la CIA, de la NSA, et des services secrets de nombreux pays de la planète, notamment français, cette startup est connue pour une utilisation massive des algorithmes et des données privées pour aider ses clients à créer de la valeur "

« Le gouvernement avance l'effacement des données de plus de 15 jours et un code informatique rendu public pour rassurer. Encore une fois les promesses n'engagent que ceux qui y croient. L'histoire récente ne joue pas en sa faveur sur le sujet. Les lois d'exception votées suite aux attentats de 2015 se sont retrouvées à caractère permanent avec un dispositif de contrôle de la totalité des communications de la population. Des boîtes noires algorithmiques sont depuis reliées à tous les opérateurs télécoms fournissant au ministère de l'intérieur des renseignements sur les individus ayant un comportement considéré comme suspect » **(4)**

« A partir du 11 mai, l'objectif est que tous les cas contacts soient testés. Cette règle exige des moyens considérables et d'abord humains. Dans ce cadre « un consortium européen a lancé le développement d'un outil numérique de suivi de contacts. Ce sera un outil complémentaire des autres moyens » a déclaré le Premier ministre. Notamment dans le cas où il faudra surmonter la difficulté de reconstituer les chaînes de transmission en zones denses, par exemple dans les transports en commun…. » (Allocution du Premier Ministre) (**2)**

Rappelons d'ailleurs que la connexion au réseau cellulaire demande nécessairement une triangulation, qui permet de vous localiser à quelques dizaines de mètres près…

Petit tour du monde des pratiques de tracking social -non exhaustif - (4)

Taïwan

Dès Janvier 2020 contrôle de température. Tous les cas suspects sont alors assignés à résidence en isolement avec contrôle du signal de leur téléphone afin de garantir que l'appareil ne quitte pas le domicile. Plusieurs appels sont par ailleurs passés chaque jour par les services de sécurité de manière aléatoire pour s'assurer que les habitants infectés sont bien chez eux.

Chine

A l'origine de la propagation du virus, la Chine a très rapidement utilisé son impressionnant arsenal technologique pour pister les cas de contamination à travers le pays. Chaque citoyen s'est vu assigner un QR code changeant de couleur (rouge/vert) en fonction du risque contagieux de l'individu. Calculé par algorithme de manière opaque .Ce code couleur est par ailleurs relié au système national de reconnaissance faciale s'appuyant sur plus de 300 millions de caméras de surveillance à travers le pays. Couplées à des capteurs thermiques dans les foyers d'infections, ces caméras permettent aux autorités de détecter et traquer par géolocalisation des smartphones tout cas suspect ou de surveiller les comportements des citoyens…

Corée du Sud

les autorités ont juridiquement un droit total d'accès aux données privées des citoyens en cas de risque sanitaire depuis l'épidémie de SRAS. Chaque personne infectée est géolocalisée par l'intermédiaire de son téléphone pour s'assurer du bon respect de son isolement…

Hong Kong

Dès l'atterrissage un bracelet électronique est remis à chaque passager par les autorités. Couplé à une application qu'il a obligation de télécharger, chaque individu est ainsi traqué pour s'assurer du bon respect de la quarantaine. Au delà des voyageurs, ce système s'étend désormais à tous les cas d'infection…

Pologne

Comme dans de nombreux pays à travers la planète, la Pologne impose à toute personne suspecte du fait d'une infection ou d'un risque de contagion, une quarantaine stricte de 14 jours à domicile. Elle peut alors choisir de manière libre entre le téléchargement d'une application, Home Quarantine, lui demandant de se prendre en selfie de manière aléatoire plusieurs fois par jour ou le passage des forces de l'ordre pour vérifier du bon respect de sa quarantaine

Israël

Habitué à la lutte anti-terroriste, le gouvernement a confié au Shin-Beth (services de sécurité intérieure) la lutte contre la propagation du virus. Analyse massive des données privées, géolocalisation des téléphones, utilisation
de drones et des systèmes de surveillance du pays pour traquer la population… »

« Ayant passé en revue les outils mis en place par les différents pays dans la lutte contre la pandémie, force est de constater que le respect de l'anonymat et des données privées n'est pas vraiment la priorité… » (**4)**

« …**il faut se rediriger vers les nombreuses autres solutions proposées :** production de masques, de tests, traçage de contacts réalisé par des humains, sans avoir à réinventer la roue. Leur efficacité semble tellement moins hasardeuse. Surtout, contrairement à StopCovid, ces solutions ne risquent pas de légitimer sur le long terme l'ensemble de la Technopolice, qui cherche depuis des années à rendre acceptable la surveillance constante de nos corps dans l'espace public par la reconnaissance faciale, les drones ou la vidéo automatisée… » (**1)**

Dans le cadre des mesures de déconfinement, l'Assemblée nationale débattra de StopCovid, sans toutefois voter spécifiquement à son sujet.
L'Assemblée doit exiger la fin de cette application. Rendez-vous sur cette page pour contacter les député·es. » (1)

Ce dossier a été mis au point à l'aide d'extraits de contributions de Jean-Christophe Bonis, de la quadrature du net, d'une équipe de chercheurs à l'INRIA. Les références et les liens se trouvent en dessous.
Ainsi que quelques liens vers d'autres dossiers pour approfondir le sujet :

SOURCES :

1) « STOPCOVID EST UN PROJET DÉSASTREUX PILOTÉ PAR DES APPRENTIS SORCIERS
https://www.laquadrature.net/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des-apprentis-sorciers/

https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des-apprentis-sorciers_6037721_3232.html

2) Allocution Premier Ministre
https://www.linformaticien.com/actualites/id/54285/le-premier-ministre-promet-debat-et-vote-sur-stopcovid-des-qu-elle-fonctionnera.aspx

La Quadrature du Net
https://www.laquadrature.net/2020/04/27/la-cnil-sarrete-a-mi-chemin-contre-stopcovid

4) Jean-Christophe Bonis
https://www.maddyness.com/2020/04/26/pourquoi-je-ne-telechargerai-pas-lapplication-stopcovid/

5) Chercheurs/Chercheuses INRIA
https://risques-tracage.fr/

6) CNIL
https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf