Solidaires Informatique
Union Syndicale Solidaires

# APPLICATION STOP-COVID :

## une expérimentation LIBERTICIDE, une ILLUSION technologique

Après la Chine, la Corée du Sud ou Israël, des pays où la surveillance généralisée et l'exploitation des données couplée à l'intelligence artificielle est institutionnelle, le Gouvernement Français étudie la diffusion d'une application qui permettrait de signaler une contamination et d'en informer les personnes ayant été en contact avec une personne infectée.

Voilà la promesse ambitieuse qui nous est faite : Freiner l'épidémie et permettre à chacun de nous de lutter contre la propagation de ce virus mortel en installant une application sur notre téléphone ! Devenir des héros sans effort, un peu comme nous pensons sauver l'hôpital public en applaudissant aux balcons chaque soir à 20 heures.

## une utilité limitée qui met en doute la véritable finalité de cet outil

L'utilisation de la technologie Bluetooth semble être préféré à celle du GPS. La première permet d'identifier et d'enregistrer les contacts, la seconde y ajoute la géolocalisation. La distance de connexion, la durée, les problèmes de transmission liés à la position du téléphone ou à son rangement au fond d'un sac, la nécessaire activation du Bluetooth, la puissance du signal variant d'un appareil à l'autre ou les problèmes de batterie sur-sollicitée sont autant d'éléments qui rendent hasardeux l'efficacité du système.

A cela s'ajoute la nécessité d'une diffusion extrêmement large de cette application. Mais certain.e.s ne voudront pas pour les raisons que nous expliquons ici, d'autres ne pourront pas faute de disposer de téléphone mobile, comme les seniors qui sont les plus vulnérables et les plus jeunes enfants, souvent asymptomatiques et qui ont le plus de difficultés à respecter les gestes barrières.

## Des dérives liberticides

Solidaires Informatique s'est toujours montré vigilant et critique sur les dérives de l'utilisation des données personnelles. Si le Règlement Général de Protection des Données (RGPD) a posé quelques garde-fous, ceux-ci ne résistent pas à la puissance des géants du net, GAFAM, BATU ou BATX (1) et de leurs Cloud à la croissance exponentielle (2), qui traquent d'ores et déjà et en continu nos vies, nos déplacements, nos goûts, nos habitudes, … Ces données à usage commercial dans un premiers temps, peuvent être ensuite dévoyées pour influencer nos opinions, contrôler nos actes (3).

Cette épidémie est ici l'occasion de mettre en œuvre des technologies de collectes de données à grande échelle directement par les gouvernements. Les enjeux politiques sont énormes et les dérives dangereuses car si aujourd'hui ce logiciel est mis en œuvre pour une maladie précise, quelles en seront les prochaines fonctionnalités, quels en seront les prochains objectifs ? Pour l'étude des relations sociales qu'introduit ce logiciel espion, la collecte des données est le plus compliqué. L'analyse est plus simple et ses conclusions

parfois simplistes : « Vous êtes ami.e avec l'ami.e d'un.e syndicaliste », voilà de quoi faire de vous un suspect qu'il est nécessaire de ficher sur la liste des potentiel.le.s « dangereux et dangereuses révolutionnaires ».

Enfin les failles de sécurité du système Bluetooth sont nombreuses et les risques de piratage de son téléphone et de vol de données personnelles seraient fortement accrus.

## une acclimatation sécuritaire

L'installation de cette application peut aussi faire craindre une banalisation de la surveillance étatique et l'acceptation sociale de technologies sécuritaires comme la télésurveillance ou la reconnaissance faciale que nous avions déjà dénoncées en co-signant une Tribune initiée par la Quadrature du Net en 2019 (4).

De plus, si le gouvernement a parlé du déploiement rapide de cette application, qu'en sera-t-il de la fin de son utilisation ? Nous avons toutes et tous des exemples de mesures sécuritaires mises en place dans l'urgence toujours en place aujourd'hui : Vigipirate devenu Sentinelle, la loi de renseignement de 2015, les lois liberticides de Sécurité Intérieure de 2017 (5), …

## L'idée naïve que la science nous sauvera

Enfin le déploiement de cette application permet de véhiculer la dangereuse idée d'un solutionnisme technologique qui permettrait de répondre efficacement aux crises écologiques et sanitaires, évitant d'en traiter les causes et les origines et de remettre en cause notre système de développement.

Mais construire des digues suffit-il à nous prémunir des inondations ou faut-il réellement lutter contre le réchauffement climatique et la montée des eaux ?

Ajouter quelques mètres de béton autour d'un réacteur nucléaire suffit-il pour éviter une catastrophe majeure ou faut-il abandonner cette folie pour des énergies renouvelables ?

Suffit-il de déployer une application sur un téléphone pour éviter la propagation d'un virus ou faut-il arrêter la déforestation, la destruction de la biodiversité, l'exploitation sans fin des territoires sauvages pour éviter les prochaines pandémies zoonose (6) ?

# RESISTEZ, N'UTILISEZ PAS L'APPLICATION GOUVERNEMENTALE STOP-COVID !

(1) GAFAM : Google, Apple, Facebook, Amazon, Microsoft - NATU : Netflix, Air BNB, Telsa et Uber – BATX : Baidu, Alibaba, Tencent et Xiaomi

(2) Volume des données numériques : 40 Zeta octets ($10^{21}$ octets) en 2020, soit 33 fois plus qu'en 2010

(3) on peut citer par exemple les scandales de Cambridge Analytica, ou les révélations des lanceurs d'alertes comme Edward Snowden pour le plus célèbre

(4) voir l'article sur notre site : Avec la Quadrature du net, contre la reconnaissance faciale sécuritaire

(5) Article d'Attac sur l'évolution des lois liberticide depuis 2015 : La lutte contre le terrorisme, le grand alibi d'une loi liberticide

(6) maladie qui se transmet de l'animal à l'homme. Article du courrier international : La destruction des écosystèmes par l'humain favorise l'émergence d'épidémies