«StopCovid», outil de traçage liberticide

Pour lutter contre l'épidémie de Covid-19 et les risques de contamination, le gouvernement a mis en œuvre une application sur ordiphone, « StopCovid ». La surveillance est-elle le prix à payer pour notre santé ?

Maryse ARTIGUELONG, vice-présidente de la LDH

Durant toute la période de l'état d'urgence sanitaire, la LDH a dénoncé et parfois attaqué en justice les mesures d'exception menaçant les droits et libertés, mesures dont on sait qu'elles sont amenées à durer (comme celles relatives à l'état d'urgence antiterroriste) et qui touchent de nombreux domaines : la liberté de circuler, de manifester, ou la surveillance du confinement par drones ou autres caméras…

Présentée par le gouvernement comme un des outils du plan de déconfinement, l'application mobile « StopCovid » a pour objectif de « *vous protéger, protéger les autres, et soutenir les efforts des soignants et du système de santé pour stopper au plus vite les chaînes de contamination et éviter une deuxième vague de l'épidémie de Covid-19* », et pour principe de « *prévenir les personnes qui ont été à proximité d'une personne testée positive, afin que celles-ci puissent être prises en charge le plus tôt possible, le tout sans jamais sacrifier nos libertés individuelles* »[1].

Alors que les tests de dépistage étaient rarement prescrits et que l'on manquait de masques, alors que seules les « auto-attestations » dérogatoires de déplacement et l'incroyable discipline de la majorité des individus acceptant ce confinement permettaient de ralentir l'épidémie, l'application a été présentée comme la protection de nos futures sorties. Mais le concept de surveillance par ordiphone a fait réagir de nombreux défenseurs des droits et libertés ainsi que des experts en cryptologie et sécurité informatique[2], qui ont dénoncé les risques liés à cet outil.

« StopCovid » est une application mobile dont le principe est d'enregistrer les contacts entre les individus. Ainsi, une personne testée positive à la Covid-19 peut alerter automatiquement toutes celles croisées à moins d'un mètre et pendant plus de quinze minutes, dont les ordiphones ont échangé des signaux Bluetooth dans les quinze jours. Ces dernières peuvent ainsi se faire dépister et s'isoler si nécessaire.

Le gouvernement a donc fait le choix d'un outil discriminatoire puisqu'il exclut d'emblée toute une partie de la population : seulement 44 % des plus de 70 ans possèdent un ordiphone et 14 % d'entre eux ne sont pas à l'aise avec l'installation d'une application ou l'activation du Bluetooth. Pourtant c'est cette classe d'âge qui est considérée comme la plus « à risques ». Le projet de montre connectée, dédiée à « StopCovid », ne semble lui pas avoir abouti…

Le choix d'une application de traçage de la population utilisant la technologie Bluetooth entraîne des risques d'atteinte à la protection des données personnelles, et, qui plus est, des données de santé, considérées comme sensibles et dont le traitement doit respecter les principes du RGPD[3] (consentement libre, minimisation et sécurité des données, limitation de finalité et de durée de conservation, information sur les risques…). De nombreux experts ont dénoncé ces risques.

Une fiabilité douteuse, un manque de sécurité

Concernant le repérage des contacts, le Bluetooth, qui permet à deux téléphones de communiquer, n'est pas conçu pour mesurer des distances, et sa fiabilité est fonction des performances de ceux-ci ; quand bien même ces distances seraient exactes, il ne permet pas de définir le contexte des contacts et la nature du risque (les personnes étaient-elles avec ou sans masque, à travers un plexiglas ou une fenêtre ? La proximité d'un malade ne signifie pas contagion automatique…).

Par ailleurs, concernant la sécurité, le fait de devoir activer le Bluetooth en permanence soumet toutes les données du téléphone à un sérieux risque de piratage (c'est la raison pour laquelle il est désactivé par défaut).

Le gouvernement a exigé, pour protéger l'anonymat des contacts, un système de pseudonymes servis par un serveur cen-

(1) www.economie.gouv.fr/stopcovid.

(2) https://attention-stopcovid.fr/#experts.

(3) Règlement général sur la protection des données.

(4) Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données, dénommé « StopCovid » (www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&categorieLien=id).

(5) Mise en demeure de la Cnil, 20 juillet 2020 (www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles).

(6) Commission nationale de l'informatique et des libertés.

(7) Alors que le choix de confier à Microsoft le stockage des données de santé de tous les Français constitue la plus grave atteinte à cette souveraineté (http://souverainetenumerique.fr/interview-health-data-hub-%C2%AB-le-choix-de-microsoft-est-un-contresens-industriel-%C2%BB).

(8) www.francetvinfo.fr/sante/maladie/coronavirus/coronavirus-l-ue-va-rendre-compatible-18-applications-de-tracage-nationales-mais-pas-stopcovid_4065047.html.

© DR

L'application « StopCovid », disponible gratuitement depuis le 2 juin 2020, était, à fin août, téléchargée 2,3 millions de fois, soit par 3,1 % de la population. De fait, son utilité est très discutable.

tral. Hormis le fait qu'un pseudonyme permet toujours de retrouver l'identité de la personne en question, qu'un serveur contenant toutes ces données peut exciter la convoitise de hackers mal intentionnés, le décret[4] lui-même prévoit d'informer de la « *possibilité limitée d'identification indirecte susceptible d'en résulter lorsque ces personnes ont eu un très faible nombre de contacts pendant cette période* ».

Les choix du gouvernement fragilisent les protections annoncées : « StopCovid » est téléchargé à partir des « magasins » Google ou Apple, qui peuvent ainsi collecter nos données via l'analyse de trafic. De plus, « *la première version de l'application faisait remonter l'ensemble de l'historique de contacts des utilisateurs au serveur central, et non les seuls contacts les plus susceptibles d'avoir été exposés au virus* »[5]. Ceci a été corrigé dans la nouvelle version déployée fin juin ; de même, le système « reCaptcha » de Google a été remplacé par celui développé par Orange suite à l'avis de la Cnil[6] (toutefois les utilisateurs de la première version n'ont pas été alertés de cette mise à jour).

La Cnil devra s'assurer que sa demande de limitation de durée de conservation des données, à la fin de l'épidémie, soit respectée, et vérifier leur destruction. Mais les annonces régulières de l'arrivée de nouvelles vagues font craindre une « durée illimitée ».

Au moment où les Européens recommencent à circuler, le choix du stockage sur un serveur central et le refus de la norme créée par Google et Apple, au nom d'une prétendue « souveraineté numérique nationale »[7], exclura « StopCovid » du futur système européen de recherche de contacts[8].

Une tendance au « solutionnisme numérique »

L'installation volontaire de « StopCovid » vaut consentement au traitement des données et respect du RGPD, mais nous avions alerté sur de possibles pressions pour inciter à l'installation (employeurs, fournisseurs de services, etc.). Il ne semble pas que ce soit le cas à l'heure actuelle, mais les menaces de retour de l'épidémie pourraient changer cela : le consentement ne serait alors plus libre, et le RGPD pas respecté.

En réalité l'application « StopCovid », disponible gratuitement depuis le 2 juin 2020, a été, à la fin août, téléchargée 2,3 millions de fois, soit par 3,1 % de la population. Elle a été utilisée par plus de mille personnes pour prévenir de leur contamination, informant par là-même soixante-douze personnes d'un risque de transmission. Les épidémiologistes estiment qu'un tel outil serait efficace si environ 60 % de la population l'utilisait. L'utilité de « StopCovid » est donc, de fait, très discutable. Cet échec ne devrait pourtant pas stopper l'obstination de nos dirigeants à vouloir trouver des solutions numériques, avec l'idée que celles-ci permettent de faire la même chose (ou plus !) pour moins cher. Ce « solutionnisme numérique » est amené à prospérer, car les autorités font valoir qu'elles ont besoin de grandes quantités de données pour gérer les épidémies futures, tout comme des mesures de surveillance et d'autres menaces à la vie privée ont été justifiées par le passé, notamment dans le cadre de la lutte antiterroriste.

Avec « StopCovid », on est face à une surveillance « choisie ». Accepter une atteinte à nos vies privées pour une hypothétique sécurité sanitaire repose la question plus large de l'acceptabilité de la surveillance intrusive et généralisée, au nom d'une quelconque sécurité. ●

« Le choix d'une application de traçage de la population utilisant la technologie Bluetooth entraîne des risques d'atteinte à la protection des données personnelles et, qui plus est, des données de santé, considérées comme sensibles et dont le traitement doit respecter les principes du RGPD. »