# StopCovid : la santé publique au prix de nos libertés ? Brèves observations sur l'application de traçage numérique

Ludovic Pailler

**StopCovid : la santé publique au prix de nos libertés ?**
*Brèves observations sur l'application de traçage numérique*

*Par Ludovic Pailler - Agrégé des Facultés de droit - Professeur à l'Université Jean Moulin - Lyon 3*

Dans son adresse aux français du 13 avril 2020, le Président de la république annonçait le développement d'une application de traçage numérique pour accompagner le déconfinement. Elle devrait encourager les personnes alertées à se confiner, à consulter un médecin ou à se faire tester, pour réduire la propagation du COVID-19.
La solution technologique n'aura pas d'effet miraculeux sans se conjuguer avec d'autres mesures. L'idée n'en est pas moins de transformer notre téléphone en bracelet électronique virtuel et d'instaurer, comme le promeut Taïwan, une auto-surveillance participative. Au-delà d'une défiance inter-individuelle accrue, les craintes se concentrent sur le respect de la vie privée. Le traçage suscite des débats animés dans la communauté scientifique comme la réaction des institutions nationales et européennes. La crainte d'une surveillance de masse et d'un profilage par reconstruction des parcours individuels et chaînes d'infection ternit les avantages épidémiologiques qui pourraient en être retirées.

Mais de quoi parle-t-on ? L'application gouvernementale n'existe pas encore. Son mode de fonctionnement, proche de celui de l'application proposée par un consortium d'industriels, a été dévoilée par l'institut national de recherche pour les sciences et technologies du numérique. Point de géolocalisation des individus ni de reconnaissance faciale comme dans d'autres États, mais une application adossée sur le système Bluetooth. Une fois installée, elle attribuerait à chaque téléphone des identifiants uniques et cryptés qui seront enregistrés dans l'historique des autres utilisateurs lors de passage à proximité. En cas de déclaration de contamination par un utilisateur, son historique d'identifiants rencontrés sera transmis à un serveur central. La consultation automatique et régulière de ce dernier par les applications des autres utilisateurs leur permettra alors d'être informés de leur contact avec une personne à risque.
Afin de susciter la confiance des français, cette application est annoncée reposer sur les bases du volontariat et de l'anonymat. Certes, toute obligation légale de faire usage de l'application et d'activer son Bluetooth est exclue, et c'est heureux. Mais la volonté paraît trop fragile au regard de l'enjeu. Nul ne peut nier la pression sociale qui s'exerce sur chacun d'entre nous dans ces temps de pandémie. Fonder un système intrusif sur l'illusion d'un consentement n'est pas acceptable quand sa finalité le fonde mieux. D'anonymat, il n'est ensuite pas question. Puisqu'elle confér un identifiant unique et crypté, l'application réalise une pseudonymisation qui justifie l'application du règlement général sur la protection des données.
Quelle ironie que ce soient les principes directeurs (art.5) de ce dernier (le droit de l'Union, donc) qui déjà contraignent le gouvernement à revoir sa copie pour respecter les engagements présidentiels.

La **licéité** du traitement (art.5.1.a) constitue un enjeu majeur. Elle ne peut pas procéder du consentement des personnes concernées qui manque d'être libre. Nombre de personnes installeront l'application convaincues, par eux-mêmes ou par un tiers, qu'elle subordonnera effectivement leur déplacement, leur accès aux commerces ou à leur lieu de travail. Songeons encore aux subterfuges vertueux (*nudges*) que certains suggèrent pour en encourager l'installation. Cette base est d'autant plus impensable qu'un consentement explicite serait appelé à justifier le traitement en principe interdit de données de santé (art.9.2.a). Avec cynisme, il serait contreproductif car faciliterait notamment l'exercice du droit à l'effacement des historiques d'identifiants rencontrés et de la déclaration de contamination (art.17.1.b).

Pour inscrire l'application dans le « respect de nos libertés publiques et de nos institutions démocratiques » (Adresse aux français du 13 avril 2020), restent les « motifs d'intérêt public important » ou les « motifs d'intérêts public dans le domaine de la santé » (art.9.2, g et i). Chacun requiert une base légale en droit de l'Union ou en droit interne et que le traitement soit nécessaire et proportionné. *A priori* le gouvernement français ne dispose pas d'un tel fondement (sauf à lire extensivement l'article L.3131-15 du Code de la santé publique) ni n'a pas prévu son adoption. Les autres conditions pourraient n'être que difficilement remplies.
Sur la nécessité, le doute naît de l'efficacité du traçage numérique. Outre que le mode de transmission du virus demeure incertain, l'efficacité du traçage dépend étroitement du taux, du type et du niveau de l'équipement de la population (faible chez les personnes âgées particulièrement exposées et les jeunes enfants porteurs asymptomatiques), du taux d'installation de l'application (fonction de la confiance dans la protection qu'elle garantit et de son efficacité) mais encore des critères de détection (durée et distance de proximité requise) et des ratés (absence de détection malgré la proximité, détection à travers un mur ou une vitre). Une évaluation de l'utilité de l'application après un temps d'utilisation pourrait nuancer la critique.
La proportionnalité dépend de l'architecture de l'application, du *privacy by design*. Les chercheurs en charge du développement sont divisés. Le traçage individuel serait moins intrusif qu'un suivi collectif procédant d'une agrégation de donnée telle qu'elle rendrait impossible une véritable anonymisation. Le système de traçage le plus protecteur de la vie privée, parce qu'il limite l'accès par les autorités publiques nationales ou étrangères, serait celui qui minimiserait autant que possible la quantité de données traités sur des serveurs centraux. Avec le système envisagé en France, seuls les historiques d'identifiants de l'utilisateur malade sont transmises à un serveur central, ce qui n'exclut pas tout recoupement propre à établir le graphe social d'un utilisateur. Le système DP-3T (*Decentralized Privacy-Preserving Proximity Tracing*), qui a les faveurs d'Apple et Google mais encore des institutions européennes, serait plus protecteur. Toutes les données demeureraient dans la mémoire du téléphone de la personne concernée ; seule transiterait par un serveur central l'identifiant de la personne infectée, ce qui rend plus difficile d'en tirer d'autres enseignements que le nombre d'utilisateurs infectés et un rythme de propagation. Reste à garantir la **sécurité** des données enregistrés sur les téléphones individuels plus exposés aux attaques.

Le principe de **transparence** implique que la personne concernée soit informée en des termes clairs et simples, accessibles et facile à comprendre, de l'identité du responsable de traitement (le ministère de la santé ?) et des finalités de ce dernier (voir *infra*). Au-delà, la publication du code source est souhaitable. C'est la condition d'une évaluation constructive de l'application par des tiers qualifiés.

L'application ne pourra poursuivre qu'une **finalité limitée** : alerter les utilisateurs sur leur proximité avec une personne infectée. Toute utilisation des données à d'autres fins devrait être explicitement écartée, sauf à ce que les données puissent être véritablement anonymisées pour dresser une cartographie de la pandémie.

La **minimisation** des données traitées implique une absence d'identification des utilisateurs par leur nom, prénom, sexe ou date de naissance ou même la collecte de données relatives à l'appareil utilisé. La pseudonymisation suffit aux finalités de l'application. Devraient être exclus le traitement de la date et de l'heure du contact à risque pour éviter la chasse aux sorcières. Mais faut-il traiter la durée et la distance approximative entre les deux téléphones pour calculer un risque de contamination, si tant est ce que soit médicalement possible ?

**L'exactitude** des données est une difficulté majeure. Le risque d'alerte pour des cas faussement positifs, résultat notamment d'un autodiagnostic, pourrait considérablement nuire à l'utilité du traçage. Une information claire sur les conséquences d'un signalement et d'un faux signalement au pénal comme au civil ne serait pas suffisante. Il est essentiel que toute entrée relative à l'infection d'un utilisateur soit subordonnée à la transmission par un médecin d'un code unique, décorrélé de tout élément d'identification, qu'il s'agisse de déclarer une suspicion, de la confirmer ou de l'infirmer par le résultat d'un test.

La **limitation de la conservation** des données exige que l'application n'ait qu'une existence provisoire, pour le temps que dure la pandémie sur le territoire français (aligné sur le temps de l'urgence sanitaire ?). Dans cette période, les données collectées ne doivent être conservées que pour le temps strictement nécessaire à la finalité de l'application. Sur chaque téléphone, l'historique des identifiants rencontrés ne devrait être enregistrés que pour la durée d'incubation du virus. Sur les serveurs, l'historique ou l'identifiant devrait être effacé automatiquement après l'écoulement d'un délai propre à permettre la diffusion de l'alerte à l'ensemble des utilisateurs concernés, sauf à ce qu'il soit conservé pour une période plus longue mais de façon anonyme à des fins statistiques.