La crise sanitaire ne justifie pas d'imposer les technologies de surveillance

Communiqué de l'Observatoire des libertés et du numérique (OLN), Paris, le 8 avril 2020,

Chacune des crises qui a marqué le 21e siècle ont été l'occasion d'une régression des libertés publiques. Les attentats terroristes du 11 septembre 2001 ont vu l'Europe adopter la Directive sur la rétention des données de connexions électroniques et l'obligation faite aux opérateurs de stocker celles de tous leurs clients. Les attentats terroristes qui ont touché la France en 2015 ont permis le vote sans débat de la loi renseignement. Ils ont aussi entraîné la mise en place de l'état d'urgence dont des mesures liberticides ont été introduites dans le droit commun en 2017.

La pandémie de Covid-19 menace d'entraîner de nouvelles régressions : discriminations, atteintes aux libertés, à la protection des données personnelles et à la vie privée…

Pour surveiller l'évolution de la pandémie, tenter d'y mettre fin et organiser la fin du confinement, les gouvernements de plusieurs pays européens proposent d'utiliser des outils numériques basés sur l'utilisation des données des téléphones portables en prenant exemple sur plusieurs pays d'Asie qui ont subi l'épidémie avant l'Europe (Chine, Corée du Sud, Taïwan, Singapour).

Deux logiques sont en œuvre : géolocaliser les populations et vérifier qu'elles respectent le confinement ; signaler aux personnes qu'elles ont pu être en contact avec des malades de la Covid-19.

En France, le 8 avril, le gouvernement a indiqué travailler sur une application pour téléphone portable, téléchargeable à titre volontaire, permettant que « lorsque deux personnes se croisent pendant une certaine durée, et à une distance rapprochée, le téléphone portable de l'un enregistre les références de l'autre dans son historique. Si un cas positif se déclare, ceux qui auront été en contact avec cette personne sont prévenus de manière automatique » [1].

Pistage des contacts (contact/backtracking)

Il est envisagé d'utiliser pour cela le Bluetooth, qui permet à deux appareils comme des téléphones portables, de se connecter lorsqu'ils sont à proximité[2]. Une application à installer (volontairement ou pas) permet aux porteurs de la Covid-19 de se signaler pour que les personnes ayant été à leur proximité soient informées sur leur téléphone portable qu'elles ont peut-être été en contact avec un porteur du virus, et qu'elles devront à leur tour rester confinées pour limiter la chaîne de contamination.

Quels sont les risques et les garanties nécessaires ?

Le Président de la République ayant déclaré que nous étions en guerre contre le virus, les mesures de restrictions des libertés nous sont présentées comme autant d'armes légitimes contre la pandémie.

Néanmoins, les utilisations envisagées de nos données personnelles (applications utilisant le Bluetooth pour le suivi des contacts) ou déjà mises en œuvre (géolocalisation) constituent une grave atteinte à nos libertés et ne sauraient être autorisées, ni utilisées sans notre consentement.

Pour que des données aussi sensibles puissent être utilisées légalement, **nous devrions être informés du moment où ces données sont anonymisées, notre consentement devrait nous être demandé, des informations faciles à lire et à comprendre devraient nous être fournies pour permettre un consentement libre spécifique et éclairé. Des garanties devraient également être fournies sur les techniques utilisées pour rendre impossible leur ré-identification**.

Concernant les applications de suivi des contacts, elle sont présentées comme peu dangereuses pour la confidentialité des données personnelles puisqu'il y aurait peu de collecte de données, mais essentiellement des connexions par Bluetooth d'un téléphone à un autre. C'est oublier que la notion de consentement libre, au cœur des règles de la protection des données, est incompatible avec la pression patronale ou sociale qui pourrait exister avec une telle application, éventuellement imposée pour continuer de travailler ou pour accéder à certains lieux publics. Ou que l'activation de ce moyen de connexion présente un risque de piratage du téléphone. Il est par ailleurs bien évident que l'efficacité de cette méthode dépend du nombre d'installations (volontaires) par les personnes, à condition bien sûr que le plus grand nombre ait été dépisté. Si pour être efficaces ces applications devaient être rendues obligatoires, « le gouvernement devrait légiférer » selon la présidente de la CNIL[3]. Mais on imagine mal un débat parlementaire sérieux dans la période, un décret ferait bien l'affaire ! Et qui descendra manifester dans la rue pour protester ?

L'atteinte au **secret médical**, à la **confidentialité des données de santé**, est aussi mis en cause, car ces applications offrent une possibilité d'identifier les malades et de les stigmatiser. Et qu'en sera-t-il de toutes les personnes qui n'auront pas installé l'application, seront-elles soupçonnées d'avoir voulu cacher des informations ?

Quant à celles qui ne possèdent pas de téléphone portable, elles risquent de subir une **discrimination supplémentaire**. Selon le CREDOC, seulement 44 % des « plus de 70 ans » possèdent un téléphone portable tandis que 14 % des Français ont des difficultés pour passer des appels ou envoyer des SMS[4]. De là à installer une application et en comprendre les alertes… Faudra-t-il les équiper d'un bracelet ou autre appareil électronique ?
Dès lors, l'atteinte au respect de la vie privée et au secret médical est susceptible d'être disproportionnée compte-tenu de l'inefficacité de la mesure en matière de santé publique.

En matière de lutte contre la pandémie et notamment de fin de confinement, il semble que le gouvernement tente de masquer ses manques et ses erreurs avec des outils technologiques présentés comme des solutions miracles. Et alors que leur efficacité n'a pas été démontrée, les dangers pour nos libertés sont eux bien réels.

Organisations signataires membres de l'OLN : Le CECIL, Creis-Terminal, Globenet, La Ligue des Droits de l'Homme (LDH), La Quadrature du Net (LQDN), Le Syndicat des Avocats de France (SAF), Le Syndicat de la Magistrature (SM)

—

[1]https://www.lemonde.fr/planete/article/2020/04/08/stopcovid-l-application-sur-laquelle-travaille-le-gouvernement-pour-contrer-l-epidemie_6035927_3244.html

[2]Technologie de réseaux sans fils d'une faible portée (10 à 100 mètres…) permettant de relier des appareils entre eux sans liaison filaire. Ils sont capables de se détecter sans intervention humaine s'ils sont à portée l'un de l'autre.

[3] Interview par l'AFP de la présidente de la CNIL, Marie-Laure Denis le 4 avril 2020 Question: Le gouvernement a-t-il la possibilité d'imposer ce type d'app, ou d'autres app visant à imposer le respect du confinement ?

Réponse: En France, les pouvoirs publics ont exclu à ce jour l'éventualité d'un recours à un dispositif obligatoire.

S'il devait en aller autrement, il serait nécessaire d'adopter un texte législatif pour mettre en œuvre ces dispositifs qui devraient en tout état de cause démontrer leur nécessité pour répondre à la crise sanitaire ainsi que leur proportionnalité par un respect des principes de la protection des données personnelles: la minimisation des données collectées, des finalités qui doivent être explicitées et précises, un caractère provisoire…

[4]https://www.credoc.fr/publications/barometre-du-numerique-2019