Conférence des évêques de France
FAMILLE ET SOCIÉTÉ

Juillet 2020 – n° 172

Numérique et lutte contre la Covid-19

Cette note propose une réflexion sur l'utilisation du numérique et le rôle des GAFAM dans la lutte contre la pandémie. Ce qui est en jeu : la souveraineté des États et la possibilité de passer de la géolocalisation des personnes au suivi des rencontres interpersonnelles.

Étant donné le mode de propagation et la virulence du nouveau coronavirus, la lutte contre la Covid-19 a soulevé partout la question des procédures et des outils réglementaires, médicaux et techniques à mettre en œuvre. Cette note a pour objet de faire le point sur les conséquences techniques et éthiques des démarches et solutions retenues.

De nombreux pays ont fait appel aux techniques numériques pour effectuer un traçage de la pandémie, avec une efficacité différente selon les contextes nationaux : habitude de respecter les règles, tradition individualiste, société soumise à diverses formes de contrainte. Certains gouvernements, en général les moins démocratiques, ont poursuivi et amplifié à l'occasion de cette crise sanitaire le développement des méthodes de contrôle social et de surveillance des citoyens.

Le recours au numérique dans la lutte contre la pandémie relève d'une éthique de responsabilité.
La question de l'intérêt et de l'efficacité du numérique pour renforcer la lutte contre la Covid-19 s'est progressivement imposée en Europe. L'Allemagne, la France et le Royaume-Uni avaient fait le choix de développer ensemble un outil numérique, mais cela n'a pas abouti.

En France, le repérage numérique des chaînes de transmission du virus dans les espaces publics a été jugé intéressant, mais le traçage des contacts qu'il implique a soulevé des contestations dès son annonce. Les tensions entre protection de la santé / défense des libertés / intérêt général / utilisation du numérique ont immédiatement fait surface. Des avis ont été demandés au CNPEN (Comité national pilote d'éthique du numérique, sous l'égide du Comité consultatif national d'éthique), à la CNIL (Commission nationale de l'informatique et des libertés), à la Commission nationale du numérique et à la CNCDH (Commission nationale consultative des droits de l'homme)[1]. Le choix du gouvernement français de déployer un outil, désigné par StopCovid, a été validé par le parlement le 27 mai 2020, pour une durée limitée, en complément des autres mesures

1. Voici les références des différents avis :
- Comité national pilote d'éthique du numérique (CNPNE), *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, Bulletin de veille n°1 du 7 avril 2020 : https://www.ccne-ethique.fr/sites/default/files/publications/bulletin-1-ethique-du-numerique-covid19-2020-04-07.pdf
- Contribution du Comité consultatif national d'éthique (CCNE), *Enjeux éthiques face à une pandémie - COVID-19* : https://www.ccne-ethique.fr/sites/default/files/reponse_ccne_-_covid-19_def.pdf
- CNIL, Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf
- CNCDH, Avis sur le suivi numérique des personnes, 28 avril 2020 : https://www.cncdh.fr/sites/default/files/avis_2020_-_3_-_200424_avis_suivi_numerique_des_personnes.pdf
- Avis du Conseil national du numérique du 23 avril 2020 : https://www.vie-publique.fr/sites/default/files/rapport/pdf/274177.pdf

SERVICE NATIONAL FAMILLE ET SOCIÉTÉ (SNFS) - Pôle Société
58, avenue de Breteuil - 75007 Paris - Tél. 01 72 36 69 09 – snfs@cef.fr

pour lutter contre la pandémie, étant précisé que cette solution ne doit en aucun cas permettre une surveillance individuelle des citoyens.

Soulignons cependant que, si le citoyen défend à juste titre la liberté face à la puissance de l'État, notamment à cause d'éventuelles dérives dans le domaine régalien, de son côté le consommateur se protège peu. Le citoyen-consommateur fait largement cadeau aux grands opérateurs privés (les GAFAM notamment) d'informations personnelles sur ses déplacements et sa santé. Mais de nombreux internautes n'en ont pas au fond vraiment conscience ou préfèrent céder à la facilité.

En Europe, la décision d'utiliser l'application nationale de traçage est laissée à l'appréciation de chaque citoyen (« en me protégeant, je protège les autres »). Typiquement, l'utilisateur sera prévenu s'il a croisé des personnes qui se seront signalées contagieuses, il pourra à son tour prendre les mesures nécessaires. On en appelle à l'esprit de responsabilité des personnes pour identifier et bloquer les chaînes de transmission du virus. L'outil est une aide et non une obligation. **La stratégie sanitaire appuyée sur le traçage numérique libre n'a donc de sens que si elle est comprise par une majorité de citoyens.** On est bien dans un choix d'éthique de responsabilité, dans une recherche du bien commun. Cela pourrait s'avérer très utile, même en France, au-delà du faible taux d'adoption actuel, en cas de reprise de la pandémie.

Plusieurs points posent question.

Quant au choix des solutions et au rôle des acteurs

1. Au niveau technique, les applications utilisent les smartphones des citoyens et leur fonction Bluetooth de transmission radio de proximité. Or l'utilisation du Bluetooth dépend des fabricants au niveau matériel et logiciel. En refusant de coopérer et de déverrouiller dans son système d'exploitation (iOS) certaines fonctionnalités de gestion du Bluetooth, **Apple a volontairement gêné les solutions imaginées par le consortium européen**[2] et affaibli la performance de l'application sur les i-phones (le Bluetooth peut s'arrêter quand le téléphone se met en veille, sans que l'utilisateur s'en rende compte, ce qui peut empêcher de détecter certains contacts proches qui auraient dû l'être).

2. Parallèlement, Apple et Google ont fait conjointement aux gouvernements une proposition de solution[3] qui remédie (au moins partiellement) aux problèmes liés au Bluetooth.

   Dans cette solution, dite abusivement « décentralisée », un serveur central contient les coordonnées téléphoniques des personnes qui utilisent l'application. Il contient aussi la liste des pseudos des personnes contaminées, que le serveur diffuse à tous les utilisateurs de l'application[4]. Un des intérêts pour Google et Apple est de pouvoir collecter à leur profit de nouvelles données liées à la Covid (bien que le RGPD[5] devrait l'empêcher partiellement), qui viendraient s'ajouter aux données de santé qu'elles collectent déjà, via les messageries et les plateformes, ou via des accords avec des réseaux hospitaliers, pouvant être vendues à des industriels, des assureurs, des laboratoires ou alimenter des outils de diagnostic basés sur l'intelligence artificielle.

   La solution de Google-Apple soulève des questions de confidentialité et de souveraineté en matière de données sanitaires.

   Notons que les codes informatiques des interfaces (les API) sont la propriété exclusive de Google et d'Apple. Les États ou les citoyens n'y ont donc

2. Apple a refusé de déverrouiller la fonction de gestion de l'économie d'énergie consommée par le Bluetooth, empêchant ainsi à certaines applications de fonctionner en permanence.
3. Apple et Google ont développé un modèle utilisant une nouvelle interface non publiée (qu'on désigne par API, *Application Programming Interface* ou interface de programmation d'application) pour la gestion du Bluetooth.
4. Dans la solution commune Google-Apple, dite décentralisée, la liste des pseudos des personnes contaminées est diffusée par un serveur central à tous les smatphones équipés. Si je suis infecté, je le signale au serveur central, la mise à jour de la liste est diffusée à tous les smartphones. Chaque utilisateur peut ainsi vérifier s'il a approché une personne infectée.
   La gestion des personnes contaminées est assurée par Google ou Apple. Ces entreprises donnent aux autorités publiques les identifiants techniques des personnes qui auront été en contact avec le virus. Les pouvoirs publics pourront alors leur envoyer, par le biais de l'application, un message avec les consignes de leur choix : aller voir un médecin, s'autoconfiner…
5. RGPD : *Règlement général sur la protection des données.* Ce texte élaboré initialement en France par la CNIL, a été adopté en 2016 par la Commission européenne et devenu applicable dans l'ensemble des États membres de l'Union européenne à compter du 25 mai 2018. Il a été repris depuis par d'autres pays.

pas accès pour en comprendre et en vérifier le fonctionnement.

3. Côté français, l'application StopCovid a été conçue de manière à garantir l'anonymat et la protection des citoyens, dans le cadre de la loi d'urgence sanitaire votée par le parlement. Cette solution est dite abusivement « centralisée » car les contacts Covid (moins d'un mètre pendant plus de 15 mn) anonymisés sont transmis à un serveur central. La gestion des personnes contaminées est effectuée dans le système d'information du ministère de la Santé et non dans l'application[6]. L'utilisateur de StopCovid sera prévenu s'il a croisé des personnes qui se sont volontairement signalées à l'application comme étant contagieuses, sans qu'on puisse savoir ni où, ni quand, le tout de manière anonyme.

   Le code informatique de StopCovid est ouvert et accessible à tous.

4. L'Allemagne et dorénavant le Royaume-Uni, entraînant par la suite d'autres pays, ont finalement adopté la solution Apple-Google. **La France au contraire a maintenu son choix pour des raisons de souveraineté en matière de données de santé.**

   De nombreux observateurs ont critiqué le choix allemand qui a été vu comme un renoncement face aux GAFAM, affaiblissant la position européenne (*cf.* par exemple l'éditorial du journal *Le Monde* du 14 mai 2020[7]). Au-delà des questions techniques, des pressions indues ont-elles eu lieu ?

   Malgré la décision initiale de travailler ensemble, **le chacun pour soi a donc pris le dessus sur la coopération et constitue une rupture de solidarité européenne en matière de protection des données sanitaires.** Et de ce fait, l'interfonctionnement des outils de traçage de la pandémie entre pays européens et la France est devenu plus difficile.

Finalement, c'est le schéma classique de positionnement stratégique des opérateurs d'internet qui l'a à nouveau emporté : Google et Apple ont mis en place des plateformes qui font interface entre les États et les utilisateurs des outils de lutte contre la pandémie, ce qui leur permet a priori de collecter les données de santé et conforte leur pouvoir face aux États. On a appliqué (par facilité ?) le *deal* classique « service contre données ». La France a rejeté cette situation qui installe Google et Apple au sein des systèmes d'information sanitaires publics.

Quant aux enjeux éthiques au niveau de l'utilisation du numérique

Au-delà des questions de souveraineté signalées ci-dessus, l'architecture de la solution promue par Google-Apple leur permet de franchir une nouvelle étape dans la capacité de suivi des individus. Cela peut avoir des conséquences importantes pour l'avenir.

En effet, là où les smartphones permettaient aux GAFAM de géolocaliser des personnes donc de tra-

6. Globalement, il y a trois composantes dans l'organisation mise en place en France : le système d'information StopCovid qui comprend les smartphones et un serveur central ; le système d'information DEP (dépistage) non connecté au précédent et dans lequel les médecins généralistes signalent les infections ; et Contact Covid, fichier connecté à DEP mais non connecté à StopCovid, qui est utilisé par les brigades sanitaires pour suivre les personnes signalées comme infectées suite aux tests, les accompagner et les conseiller.
   Chaque citoyen est libre d'installer ou non sur son smartphone cette application basée sur un protocole appelé « Robert ». L'identité du propriétaire du smartphone ou l'identification du smartphone sont inaccessibles et remplacées par des pseudos, identifiants anonymisés et cryptés, générés aléatoirement, mis à jour régulièrement. Si deux personnes équipées de l'application se croisent pendant 15 mn au moins dans un rayon approximatif d'un mètre, leurs pseudos (sans lieu ni datation) sont enregistrés dans leurs smartphones respectifs pendant 15 jours. Cela est vérifiable car le code informatique de StopCovid est ouvert et accessible à tous.
   Périodiquement les smartphones équipés communiquent à un serveur central les pseudos des « contacts », c'est-à-dire des personnes qui se sont croisées dans ces conditions. En retour, le serveur indique au smartphone si des personnes parmi celles qui ont été croisées sont contaminées, sans autre information (ni pseudo, ni lieu, ni date).
   En effet, toute personne qui a été testée positive au virus peut le signaler sur son téléphone grâce à un code qui lui a été fourni avec le résultat du test. Les personnes qu'elle a croisées au cours des 15 jours précédents seront alors informées qu'elles ont croisé une ou des personnes testées positives (sans savoir qui ni où ni quand) et qu'elles sont à risque.
   Elles peuvent alors contacter une brigade sanitaire pour faire le point, elles doivent se confiner à leur tour et consulter leur médecin.
   L'objectif est bien, à l'initiative des citoyens, de repérer et bloquer plus rapidement les chaînes de transmission.
7. « L'Europe doit tracer la contamination du Covid-19 sans Google et Apple. L'incapacité des Européens à s'entendre sur un système commun d'identification des personnes côtoyées par les malades et l'entrée en scène des GAFAM risquent d'aboutir à des résultats désastreux. »

cer leurs déplacements (ce qui est très largement utilisé par exemple par les services Waze ou bien Google Maps, qui sont tous les deux sous contrôle d'Alphabet, la maison-mère de Google) puis d'utiliser ces données pour sélectionner les informations et publicités à leur adresser, ils disposent dorénavant du moyen de tracer les rencontres entre les personnes, ou leur passage devant un objet équipé d'un Bluetooth. Grâce à l'interface Bluetooth qu'ils ont développée, la mise en œuvre de ces fonctions est sous leur contrôle.

On passe ainsi de la géolocalisation des personnes (qui, où et quand) à un suivi des contacts interpersonnels de proximité (qui, où, quand, avec qui), c'est-à-dire au suivi des relations entre personnes. **On franchit une nouvelle étape dans l'utilisation du numérique en ouvrant la voie au suivi des personnes dans leur vie relationnelle, leurs réseaux et leurs activités.** Cela peut déboucher, par la seule décision de Apple ou Google, sur des usages nouveaux, des applications commerciales, etc., mais aussi un jour sur de nouvelles fonctionnalités de contrôle.

Qui décidera d'autoriser ou non ce suivi des relations interpersonnelles ? Qui en fixera les règles ?

Une telle question mériterait d'être soulevée, les règles d'usage étant de fait aujourd'hui établies par ces entreprises privées multinationales.

La souveraineté des États et de l'Europe versus le pouvoir des GAFAM

Ce sont les fabricants de terminaux et non les États qui maîtrisent les fonctions embarquées dans les smartphones et leur usage, ainsi que la mise à jour des systèmes d'exploitation et la diffusion des applications (*cf.* Play Store de Google et App Store d'Apple). Ils peuvent donc s'en réserver certains usages, en ne donnant pas accès aux API *ad hoc* (*cf.* note 3), même en cas d'urgence, sanitaire notamment[8].

Il y a donc là-aussi un problème de souveraineté : les États n'ont pas la maîtrise d'outils qui ont de plus en plus d'importance stratégique, alors qu'ils peuvent par ailleurs interdire, via la normalisation, la vente de jouets dangereux par exemple…

Quelle entité publique a eu connaissance des caractéristiques techniques de la nouvelle API Bluetooth déployée par Google et Apple ? À l'avenir, qui en Europe fixera ou contrôlera les caractéristiques techniques des terminaux autorisés ? En France, cela pourrait relever de la CNIL ou de l'ARCEP (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). On le fait depuis longtemps pour les automobiles ou les normes des équipements électriques… comme pour les jouets d'ailleurs, ce qui se comprend.

Une réaction concertée des européens semblerait justifiée.

Bernard Jarry-Lacombe
Groupe de travail « Innovation et société »,
Service national Famille et société

8. Sauf à « forcer » l'installation de logiciels, ce qui serait difficile pour un déploiement en masse car requérant une compétence technique d'installation.