Epidémie, numérique et libertés publiques

La crise épidémique actuelle constitue une nouvelle occasion de remettre en cause les équilibres auxquels parviennent les sociétés entre les aspirations, souvent contradictoires, à la liberté d'une part et à la sécurité de l'autre. C'est ce à quoi nous avons assisté il y a quelques années avec la multiplication des attentats de l'Etat Islamique en Europe. Une société qui a peur est généralement prête à accepter une réduction des libertés publiques. Dans une certaine mesure, cela peut se comprendre. Cependant, l'expérience montre que les mesures restrictives de libertés, toujours présentées comme exceptionnelles et limitées dans le temps, finissent immanquablement par devenir générales et pérennes. Par ailleurs, conjuguées à un discours politique démagogique (commode pour ceux qui exercent le pouvoir, et plus encore pour ceux qui aspirent à s'en emparer), elles font naître au sein des populations une frustration sécuritaire et une fuite en avant qui ne permettra évidemment pas d'atteindre l'objectif du risque zéro, par nature hors de portée.

Toutefois, sauf à verser dans un déni suicidaire, il faut bien reconnaître également que la raison commande, en temps de crise, de prendre certaines mesures pour protéger les populations. Rassurer à tout prix et contre toute logique peut être aussi démagogique qu'exagérer les risques : pour s'en tenir à des faits récents, présenter le coronavirus comme une simple grippe ou prétendre que le premier tour des élections municipales pouvait être maintenu sans inconvénient s'est avéré mensonger et préjudiciable, pour ne pas dire davantage.

Comme on le voit, une crise de cette nature, dans laquelle les avis scientifiques sont eux-mêmes divergents, plonge les décideurs politiques dans des problématiques d'une grande complexité. Dans une situation aussi riche en données, seule la réflexion collective, éclairée par l'information la plus complète possible, permet, non pas nécessairement de prendre les bonnes décisions (ce qui ne peut être vérifié qu'après coup), mais les décisions les plus raisonnables en l'état du niveau d'information dont on dispose.

S'agissant de l'atteinte aux libertés publiques, leur caractère difficilement réversible – que nous soulignions précédemment – impose la plus grande vigilance.

Aussi, les mesures actuellement proposées relatives à l'exploitation la plus avancée des moyens numériques (*tracing, tracking,* etc.), ne relèvent pas seulement de la gestion de la crise actuelle mais

risquent de marquer durablement et significativement nos modes de vie et nos libertés. Elles ne peuvent être prises à la sauvette par un gouvernement, quelle que soit la confiance ou la défiance dont il est l'objet.

Par ailleurs, il n'existe aucun mouvement général et planétaire inéluctable rendant dérisoire la résistance de communautés réfractaires. Chaque collectivité humaine conserve son libre-arbitre collectif. Nous ne citerons ici à titre d'illustration que le refus par certaines villes américaines des caméras à reconnaissance faciale.

C'est la raison pour laquelle nous avons souhaité ouvrir pleinement en Corse le débat public sur les mesures actuellement en gestation.

Jean-Guy Talamoni

Rapport du Président de l'Assemblée de Corse visant à l'ouverture d'un débat public

Covid-19 : les libertés publiques à l'épreuve du traçage numérique

INTRODUCTION

La crise pandémique que nous traversons a mis en avant un manque de préparation très important, conduisant la moitié de la planète à devoir se confiner, abandonnant par-là ses libertés les plus fondamentales, notamment celles d'aller et venir ou encore de se réunir. Pour répondre à ce manque d'anticipation, on a vu les gouvernements, mais aussi la société civile s'appuyer sur la technologie dans le but de satisfaire une demande pressante, urgente. En cette période de crise, on se tourne vers :

- la technologie scientifique d'abord : mener des recherches,
- la technologie industrielle pour produire en quantité et rapidement des protections (masques, respirateurs…).

La technologie de l'information est également mise en avant. Les nouveaux outils numériques sont utilisés pour toutes sortes de raisons, notamment l'intelligibilité des chaines de transmission du virus avec les datas de chaque gouvernement, partagées en temps réel. Tous les pays qui en ont la possibilité cherchent aujourd'hui à utiliser des outils permettant de contenir l'épidémie, notamment en passant par une forte prévention, mais qui, pour certains, présentent une frontière ténue avec des tendances à la répression.

En France, par exemple, les forces de l'ordre ont utilisé des drones pilotés à distance, équipés de haut-parleurs et de caméras pour dissiper les rassemblements et faire respecter le confinement, malgré un certain flou juridique autorisant cette utilisation.

Les technologies sont aujourd'hui présentées comme pouvant nous aider à reprendre une vie normale en s'assurant de ne pas être un danger pour les autres.

L'option au cœur de l'actualité est l'utilisation d'applications qui permettent d'alerter les personnes susceptibles d'être des cas-contacts pour qu'elles se dépistent, et observent une période d'isolement afin de casser les chaines de contamination et nous préserver de rebonds épidémiques. Une solution rapide, accessible, simple d'utilisation.

Dans certains cas on parle de "tracking" (application utilisant la géolocalisation des malades), dans d'autres, de "tracing" (application utilisant la technologie Bluetooth, présentée comme plus respectueuse de la vie privée des utilisateurs).

La France, comme d'autres pays européens, a lancé une réflexion sur l'élaboration d'un nouvel outil : l'application "Stop Covid". Les initiatives prises par les Etats membres sont soutenues par l'Union Européenne. Elle leur apporte son concours en édictant des orientations et en incitant les pays à travailler de concert, pour dessiner les contours d'applications qui puissent communiquer entre elles et proposer un tracing au-delà des frontières, tout en respectant les règlements de protection des données.

La discussion est ouverte, les protocoles sont en évolution et beaucoup d'inconnues sont encore à lever. Rien aujourd'hui n'est arrêté, pas même l'éventuelle mise en service d'une telle application, bien qu'une première version serait prête pour le 2 juin selon le Secrétaire d'Etat au Numérique. Cela fera l'objet d'un débat parlementaire lorsqu'il s'agira d'envisager son utilisation.

Nous avons cependant quelques éléments et données sur lesquels appuyer un début de réflexion concernant l'utilisation de tels outils et les conséquences qui peuvent en découler. Car l'Histoire nous apprend que certaines décisions prises dans l'urgence ont entrainé des situations auxquelles on ne s'attendait pas et ont conduit parfois à une perte de contrôle.

Il convient donc de bien peser les tenants et les aboutissants de ces avancées numériques ainsi que d'évaluer au plus près leurs potentielles dérives avant de lancer leur utilisation. Cela relève des sujets dont les autorités publiques doivent s'investir.

I. CRISE DU COVID ET DÉCONFINEMENT : LE NÉCESSAIRE SUIVI ÉPIDÉMIOLOGIQUE

A. LE CONTACT TRACING : UNE PRATIQUE ANCIENNE

Le "contact tracing" est une pratique ancienne, traditionnelle dans la gestion d'une épidémie. Concrètement, il s'agit d'une véritable enquête qui permet d'identifier ce que l'on appelle les "cas-contacts", c'est à dire, les individus ayant été potentiellement infectés par un cas déclaré positif. Les enquêtes de recherche de cas-contacts ont été menées pour lutter, entre autres, contre l'épidémie du Sras en 2002-2003, du Mers en 2012-2013 ou encore contre celle d'Ebola.

Aujourd'hui, la pratique se poursuit et est prévue dans les différents plans de lutte contre les épidémies. Au début de la crise du coronavirus, les autorités françaises se sont reposées sur le "plan pandémie grippale" de 2011 : dès la phase initiale (antérieure au Stade 1) correspondant au contexte général suivant : *"une information encore incertaine laisse penser qu'un nouveau virus grippal à potentiel pandémique est apparu et a commencé à se transmettre dans une population."*[1]*;* la prise en charge médicale des sujets symptomatiques (cas suspects) s'accompagne de la prise en charge des personnes ayant eu un contact avec l'individu positif (cas-contact) et l'investigation autour des cas suspects.

[1] Plan National de Prévention et de Lutte "Pandémie Grippale", 2011, page 34.

Concrètement, cela prend la forme d'une enquête réalisée par des équipes dédiées. Ces dernières sont chargées d'entrer en contact avec le patient et le questionner sur les personnes qu'il a pu rencontrer au cours des derniers jours, avec qui il aurait entretenu des liens de proximité pendant un certain temps. À charge ensuite pour cette même équipe de prévenir les cas-contacts et de leur donner une procédure à suivre qui se résumait au début de la crise à l'isolement chez soi, la prise de température récurrente, le maintien des gestes barrières et des appels fréquents aux équipes si l'individu était considéré comme présentant un risque élevé. Ces équipes ont eu aussi un rôle pédagogique important car elles ont permis de faire prendre conscience aux malades potentiels de leur responsabilité dans la chaine de transmission du virus, conduisant chacun à respecter au mieux les recommandations.

Aujourd'hui, la composition de ces équipes ou "brigades" va être élargie et elles seront hautement sollicitées dans le cadre du déconfinement.

B. DANS L'OPTIQUE DU DÉCONFINEMENT : LA NÉCESSITÉ D'EFFECTUER UN SUIVI ÉPIDÉMIOLOGIQUE COMPLET

Comme depuis le début de la crise, et encore plus à l'issue de la phase de confinement strict, il devient indispensable de détecter le plus rapidement possible les personnes potentiellement atteintes du coronavirus avant même l'apparition de leurs symptômes.

Le rapport informatif "Lutter Contre le Covid-19" présenté en Conférence des Présidents, préconisait déjà la mise en place d'un suivi épidémiologique à l'issu du confinement.

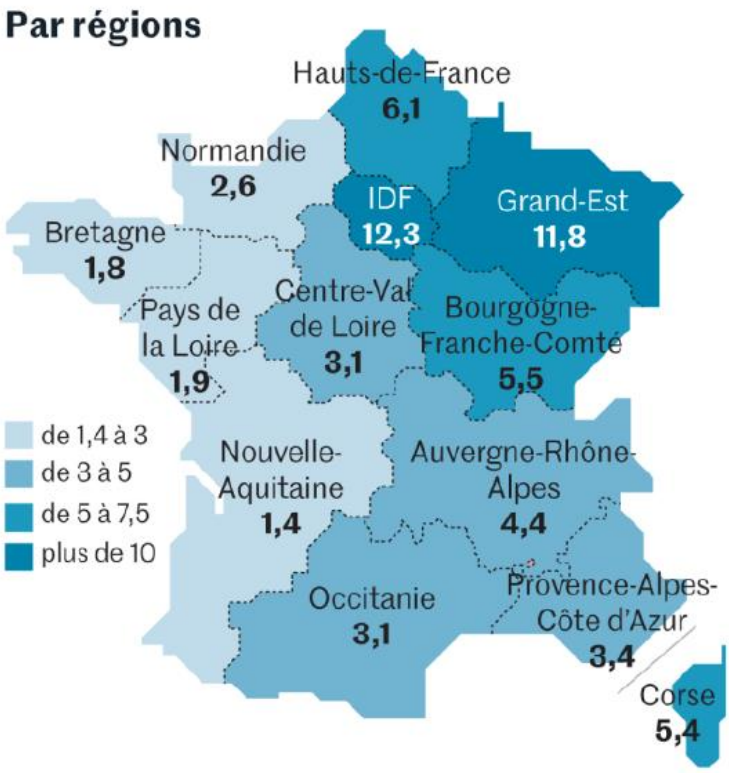
Simon Cauchemez, membre du Conseil scientifique Covid-19 présidé par Jean-François Delfraissy et responsable de l'unité de modélisation mathématique des maladies infectieuses à l'Institut Pasteur a été auditionné par la Commission des Lois de l'Assemblée Nationale le 8 avril dernier. Lors de son intervention, il a fait état de la nécessité d'identifier les cas et de suivre les contacts pour réussir la sortie du confinement et revenir à une vie quasi "normale".

Avant de conclure son exposé, Simon Cauchemez a rappelé que : "*la stratégie d'identification des cas et de suivi des contacts n'a de sens qu'une fois l'épidémie éteinte, lorsque l'on est en mesure de détecter très rapidement les personnes contaminées et de retrouver celles avec lesquelles elles ont été en contact.*"[2]

Si l'on se fie à la théorie de l'immunité collective qui veut que 66% de la population doit avoir été en contact avec le virus pour limiter sa propagation, alors même que cette immunité n'a pas encore été démontrée, il s'avère que le confinement a eu pour conséquence de ne pas permettre à ce seuil d'être atteint, comme le montre la carte ci-dessous. Pour ce qui concerne la Corse, ce taux s'élèverait à 5,4% selon une étude de l'Institut Pasteur réalisée en collaboration avec Santé Publique France et l'Inserm, à partir de modélisations mathématiques et statistiques.

S'il faut noter que ce chiffre est à relativiser compte tenu du fait qu'il n'est pas corroboré par une politique forte et ambitieuse de tests ou une enquête de séroprévalence, il est toutefois admis que le taux de contamination reste bas.

[2] http://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_lois/l15cion_lois1920051_compte-rendu



Infographie Le Monde

C'est la raison pour laquelle une seconde vague, pouvant être aussi dévastatrice que la première, reste tout de même à craindre, malgré l'accroissement des matériels médicaux et des ressources en services de réanimation, dans un contexte où les personnes qui ont renoncé aux soins pendant le confinement, risquent d'affluer dans les prochaines semaines.

Le plan de déconfinement présenté par le Premier ministre Edouard Philippe mentionne la création de "brigades de cas-contacts" chargées d'opérer un contact tracing auprès des personnes testées positives. Les personnes, agents et organismes habilités à recueillir les données sont définis aux articles 3 et 14 du décret n° 2020-551 du 12 mai 2020. Le même décret prévoit que ces brigades départementales constitueront deux fichiers différents. [3]

Le premier, nominatif, appelé Sidep recensera les données fournies par les laboratoires à la suite des tests covid-19 : nom, sexe, date de naissance, adresse, numéro de téléphone du malade, type de résidence (habitat individuel, personne hospitalisée…) et d'activité (professionnel de santé ou non). Sidep sera également utilisé dans le cadre de la surveillance épidémiologique par les autorités sanitaires, mais à partir de données anonymisées.

Le second fichier, le "Contact Covid" sera détenu par l'assurance maladie pour connaitre les personnes à contacter, les fameux "cas-contacts". Notons que ces derniers pourront récupérer gratuitement des masques et réaliser un test sans prescription médicale.

[3] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041869923 .

> "*Tout d'abord, le recueil des résultats des tests, lorsqu'ils sont positifs, par les laboratoires. Ensuite, ce qu'on appelle le tracing de niveau 1, qui sera exercé par les médecins, les professionnels de santé de premier recours (...) pour définir le premier cercle des cas de contacts potentiels. Le tracing de niveau 2, lui, sera organisé par l'Assurance maladie : il vise à enrichir la liste des contacts potentiels au-delà de ce premier cercle, de vérifier qu'aucune personne potentiellement malade n'ait pu échapper aux premiers tracings et donner des consignes prophylactiques aux intéressés. Le tracing de niveau 3 est organisé comme c'est le cas depuis le début de l'épidémie, par les Agences régionales de santé : il s'agit d'aller identifier des chaînes de contamination, des chaînes de transmission, ce qu'on appelait à un moment donné les 'clusters'. Les ARS seront aussi chargées de faire respecter les consignes sanitaires. (Enfin) la surveillance épidémiologique locale et nationale sera organisée, comme c'est déjà le cas, par Santé Publique France et la direction générale de la Santé*"
>
> – Olivier Véran, lors de la conférence de presse du 2 mai, à l'issue du Conseil des Ministres.

Il est prévu que les médecins, une fois les résultats des tests reçus, demandent à leurs patients des informations sur leurs cas-contacts via un formulaire. L'identité de la personne malade et de ses contacts seront ensuite transmises à l'assurance maladie. Il se peut que ces médecins reçoivent une rémunération pour cela.

L'extension de l'accessibilité aux données médicales à un grand nombre de personnes, pose le problème du respect des règles de confidentialité. Ainsi la loi de prorogation de l'état d'urgence, dans son article 11, tout comme le décret, ont eu besoin de délimiter précisément les organismes, les institutions et les personnes qui pourront avoir accès à ces données. L'article 14 du décret donne la possibilité aux ARS d'avoir "*recours à des sous-traitants pour exercer, les missions de réalisation des enquêtes sanitaires, d'orientation, de suivi et d'accompagnement des personnes et de surveillance épidémiologique*." Mais les ARS devront s'assurer que "*leurs sous-traitants présentent des garanties de compétence suffisantes pour assurer la mise en œuvre des mesures techniques et organisationnelles appropriées et le respect des règles de confidentialité*."

Pour encadrer les missions des brigades et éviter les risques d'abus de pouvoir, un guide pratique à leur intention est en cours d'élaboration. En cas de non-respect du secret médical, les membres des brigades pourront être sanctionnés d'une amende de 15 000 euros et d'un an de prison.

Ces différents questionnements liés à la pertinence des fichiers mis en place ont fait l'objet d'un amendement de la part du Parlement qui a ajouté au texte prorogeant l'état d'urgence sanitaire la création d'un "*Comité de contrôle et de liaison Covid-19 ».*

Ces brigades constituent une initiative énergivore en temps et en ressources humaines. Et c'est là que la technologie, en théorie, pourrait nous aider à dresser un portrait beaucoup plus précis, efficace, rapide et global sur les cas de contamination et favoriser un plan de prévention à grande échelle.

II. LA TECHNOLOGIE EN APPUI À LA GESTION DE LA CRISE

A. LA TECHNOLOGIE A ÉTÉ UTILISÉE DANS PLUSIEURS PAYS POUR LUTTER CONTRE LE COVID-19

Plusieurs pays ont répondu à la crise du Covid-19 par l'utilisation massive de technologies. Certaines plus liberticides que d'autres.

Utilisation de bracelets électroniques en Australie occidentale pour les personnes étant potentiellement atteintes de la maladie, plateformes de délation en Nouvelle-Zélande, application permettant d'attester chaque jour à la police que l'on est bien chez soi en Pologne, reconnaissance faciale à Moscou pour déterminer les personnes enfreignant leur quarantaine, caméras thermiques pour repérer les personnes fiévreuses en Chine, le tout accompagné d'un traçage et d'un code couleur permettant ou non d'accéder à certains espaces...

En ce qui concerne le tracing, la confusion sémantique avec le tracking s'entretient du fait de la diversité des dispositifs et du curseur relatif aux technologies employées, au respect de l'anonymat et de la vie privée.

En Corée-du-Sud, lorsqu'un individu a été testé positif, les habitants de son quartier en sont informés via une application qui indique son âge, son sexe, et la liste de ses déplacements récents. Cette application a donné lieu à des campagnes de dénigrement en ligne par la suite.

En Israël, l'application "Hamagen" géolocalise les porteurs du virus et informe les usagers si ceux-ci ont croisé des cas positifs. Pour ce faire, le Ministère Israélien de la Santé communique en temps réel les données sur les personnes contaminées aux utilisateurs du téléphone. Si l'usager de l'application croise un malade, il reçoit une notification.

Avec la géolocalisation, il est également possible à tous les détenteurs d'Hamagen d'éviter les espaces trop exposés au virus. En moins d'une semaine, l'application a été téléchargée plus d'un million de fois et est basée sur le volontariat. [4]

Dès le mois de mars, l'Autriche a lancé "Stopp Corona" initiée par la Croix Rouge. La personne malade se signale sur son téléphone. L'application envoie alors un message aux personnes avec qui il a été en contact les dernières 48H, sans donner le nom de la personne contaminée. Les données ne sont stockées que sur le téléphone, jamais en dehors de celui-ci, ce qui fait dire à l'ONG de Max Schrems, militant pour la protection des données personnelles, que cette application est respectueuse de la vie privée.[5] Le code-source de l'application a été rendu public pour inspirer d'autres Etats. Le fait que les informations ne sortent pas du téléphone des utilisateurs participerait grandement à instaurer une certaine confiance en l'application.

Singapour a été le premier pays à avoir lancé une application du même type, l'application Trace Together, qui propose une technologie Bluetooth, a priori respectueuse de l'anonymat et des données personnelles mais dont l'usage fut trop limité pour avoir un réel impact. Il a en revanche diffusé une fausse croyance quant à la puissance de la technologie numérique sur la protection de la santé publique. Au final, Singapour a connu une forte hausse de la contamination. En un mois, l'application de traçage, facultative et anonyme, a laissé place à SafeEntry, une application de

[4] "*En Israël, des algorithmes pour contrer le coronavirus*", L'Obs avec AFP, 31 mars 2020 (https://www.nouvelobs.com/societe/20200331.AFP5034/en-israel-des-algorithmes-pour-contrer-le-coronavirus.html).

[5] "*Coronavirus: en Autriche, pourquoi l'application de traçage numérique est saluée par les ONG*", 27 avril 2020, Radio France Internationale.

tracking, obligatoire et nominative. C'est sur le premier modèle que se penchent aujourd'hui d'autres pays européens dont l'Allemagne et la France. Pour combien de temps encore ?

B. LE PROJET D'APPLICATION STOP COVID EN FRANCE : ENTRE ESPOIRS ET CRAINTES QUANT À SON EFFICACITÉ

L'idée de créer une application a pour principaux avantages un gain d'efficacité énorme dès lors qu'elle permet de toucher des millions d'utilisateurs et qu'elle nous offre la possibilité de remonter à des personnes que l'on ne connait pas (des individus croisés à l'occasion d'un trajet dans un transport en commun, dans un centre commercial, ou tout autre lieu public).

L'application est prévue comme un outil complémentaire au plan de lutte contre le covid-19. Les premiers projets de l'application peuvent a priori être "rassurants". Les maîtres mots étant volontariat et anonymat.

Pour que l'on ne puisse pas y suspecter une volonté de surveiller massivement la population, le projet se baserait sur l'utilisation du Bluetooth plutôt que du GPS. Avec le Bluetooth, l'idée n'est pas de cartographier nos déplacements mais plutôt d'enregistrer, via des codes, les rencontres entre plusieurs individus qui se seraient tenus à une distance relativement proche.

Ainsi, deux smartphones sur lesquels l'application aura été installée, vont émettre et recevoir des codes composés de chiffres et de lettres lorsqu'ils seront proches l'un de l'autre. Ces codes représentent des identifiants qui changent régulièrement, rendus "anonymes" et stockés.

Si l'une des personnes s'avère être positive les jours qui suivent, alors le téléphone de la seconde recevra une notification indiquant qu'elle a été en contact récemment avec un cas positif, la priera de s'isoler et de se rendre dans un centre de test. En effet, après avoir effectué le test, et s'il est positif, les données de l'application sont récupérées et placées sur une liste informatique permettant de prévenir chaque cas-contact, s'il a téléchargé l'application.

Via son communiqué du 22 avril 2020, l'Académie nationale de médecine s'est prononcée en faveur de l'utilisation de smartphones pour le suivi du déconfinement.

Les conditions à la pleine efficacité de cette application

Pour que l'application puisse atteindre son objectif, d'une part, il est nécessaire de pouvoir tester en grand nombre. Sans les tests, pas d'inscription sur une liste de patients et donc, pas de prévention.

D'autre part, rien ne prouve que la technologie Bluetooth puisse fonctionner dans cette optique et que l'échange de codes entre deux téléphones soit faisable, et si elle l'est, à quelle distance elle sera efficiente.

Ensuite, il faut qu'une part importante d'individus puissent installer l'application qui ne fonctionne que sur smartphone.

Enfin, il faut qu'une large part de la population joue le jeu et accepte de suivre les règles reçues via un écran. Rappelons que le contact humain joue un rôle important dans la prise de conscience de

l'individu, d'où le possible manque d'efficacité comparé aux enquêtes épidémiologiques de terrain.

Ces différents points montrent donc que l'application, telle qu'elle est aujourd'hui conçue, ne peut se substituer aux "brigades d'enquêtes", mais doit jouer un jeu de complémentarité dans ce plan de tracing.

Ces premiers obstacles ne sont pas les seuls. D'autres, bien plus importants, pourraient menacer nos libertés individuelles.

C. DES INTERROGATIONS PRÉOCCUPANTES

De nombreux experts du monde numérique alertent contre le risque que cette application échappe à certains contrôles et soit détournée de son but premier.

Quatorze d'entre eux, experts en droit des technologies, sécurité, et cryptographie ont publié un document "*traçage anonyme, dangereux oxymore*"[6], à destination des non-spécialistes pour mettre en garde contre ces possibles dérives. En voici les principales leçons :

Résumé

– Il n'y a pas de base de données nominative des malades.	☑ VRAI
– Les données sont anonymes.	⊘ FAUX
– Il est impossible de retrouver qui a contaminé qui.	⊘ FAUX
– Il est impossible de savoir si une personne précise est malade ou non.	⊘ FAUX
– Il est impossible de déclencher une fausse alerte.	⊘ FAUX
– L'utilisation du Bluetooth ne pose pas de problème de sécurité.	⊘ FAUX
– Ce dispositif rend impossible un fichage à grande échelle.	⊘ FAUX

Deux modèles sont envisageables concernant le recueil et la centralisation des données ou "codes" émis et récupérés par les téléphones.

Un modèle dit "décentralisé" : une fois la personne testée positive, les codes de son téléphone **émis** les jours précédant celui du test, sont envoyés à l'Agence Régionale de Santé par exemple ou directement entre téléphones (pair-à-pair). Ainsi, les "téléphones contacts" sont alertés. On constitue donc ici une liste de malades.

Un modèle dit "centralisé" : une fois la personne testée positive, les listes de codes **reçus** par le téléphone ces derniers jours (cas-contacts) sont envoyés vers une autorité centrale qui est seule détentrice des informations. Dans ce cas, les téléphones envoient chaque jour les codes qu'ils ont émis pour être alertés si oui ou non, ils font partie de cas-contacts. Ici on constitue un fichier de cas-contacts.

[6] "Le traçage anonyme, dangereux oxymore - Analyse de risques à destination des non-spécialistes", version du 21 avril 2020, www.risques-tracage.fr.

Une bataille entre l'Institut national de recherche en informatique et en aéronautique (INRIA) et la Direction Interministerielle du Numérique (Dinum) a eu lieu. L'INRIA étant pro modèle centralisé via le protocole ROBERT (ROBust and privacy-presERving proximity Tracing), tandis que la Dinum plaidait pour un protocole décentralisé comme l'ont adopté l'Autriche, la Suisse, l'Estonie ou encore l'Allemagne, alors même que cette dernière a mené avec l'INRIA, la mise au point du protocole ROBERT.

Le modèle décentralisé est une option qui semble avoir été écartée de l'initiative européenne PEPP-PT (Pan European Privacy-Preserving Proximity Tracing) "v*isant à définir les lignes directrices d'une application conforme aux valeurs européennes*".

La France tend donc à mettre en place le modèle centralisé qu'elle estime plus sûr : *"Avec le système dit décentralisé, reposant sur les API d'Apple et de Google telles qu'elles sont proposées à ce stade, tout est dans les téléphones, donc sous leur seule maîtrise. Nous considérons, à ce titre, que le choix du système centralisé que nous avons retenu présente plus de garanties pour l'État et les citoyens en termes de confidentialité et de sécurité",* selon le cabinet du Secrétaire général au Numérique, qui privilégie la souveraineté de l'Etat à celle des entreprises privées (Google/Apple).

Toutefois, l'INRIA pilote le projet, entouré d'entreprises privées, qui ne sont qu'"exécutrices" selon Cédric O. Entre autres, "*Capgemini, Dassault Systèmes et Orange, ainsi que d'autres entreprises, telles que Lunabee studio et Withings, le champion français des objets connectés. À ce premier cercle de l'équipe-projet, s'ajoute un second cercle de contributeurs, certains à titre individuel, quand le reste est constitué de petites entreprises, mais surtout des principaux acteurs du numérique français : Atos, Thales et deux autres membres du consortium : Sopra Steria et Sia Partners.*"

L'anonymat

Les deux modèles, centralisé ou décentralisé, nécessitent de faire confiance à une autorité : centrale pour le premier ; régionale pour le second.

Dans les deux cas, l'anonymat peut être mis à mal : les autorités peuvent, en recoupant plusieurs données, retrouver l'identité cachée derrière les codes ; d'autre part, on sait que toute donnée informatique peut être piratée.

Dans le modèle centralisé, par exemple, l'autorité pourrait croiser les données reçues et en déduire par exemple que certaines personnes testées positives précédemment n'ont pas respecté leur consigne de quarantaine. Peut-il alors s'ensuivre des sanctions ? Car, ce qui est présenté comme un code "anonyme" n'est en réalité qu'un "pseudonyme", pouvant être désanonymisé. Les centres de recueil de ces données détiendraient donc bien des données "sensibles" relatives à la santé des individus.

Sur cette fuite des données confidentielles, il est plus préoccupant de savoir que ces données peuvent être piratées, voire rendues publiques une fois désanonymisées, que de savoir qu'elles sont détenues par une autorité de santé ou par les "brigades" si, comme il est prévu, elles sont composées de personnes soumises au secret professionnel de façon temporaire et encadrée.

Cette possible perte d'anonymat, peut aussi être le fait d'une simple déduction de la part des détenteurs de l'application. En effet, les utilisateurs eux-mêmes peuvent déduire ou suspecter parfois facilement les personnes ayant été contaminées dans leur entourage, ce qui peut donner lieu une chasse aux sorcières entre individus.

L'utilisation dérivée de cette application

La possibilité de savoir si une personne ciblée est malade ou non peut se faire très simplement, à partir d'un téléphone placé près d'elle. Cela pourrait être utilisé lors d'un entretien d'embauche par exemple. L'employeur pourra ainsi savoir si le candidat est malade entre l'entretien et la signature du contrat.

Il est également facile de déclencher de fausses alertes et faire croire à quelqu'un qu'il est peut-être malade, et ainsi le mettre hors-jeu face à une concurrence pour décrocher un poste, une compétition, ou autre. A l'inverse, une personne voulant se faire passer pour malade pourrait promener son téléphone parmi une multitude de personnes ou se procurer le téléphone d'un malade, éventuellement contre de l'argent, de sorte que son appareil reçoive une notification lui demandant de s'isoler, de cette façon elle pourrait espérer "se faire tester en priorité", "bénéficier d'un arrêt de travail", etc.

Le Bluetooth remis en question

Comme montré plus haut, il n'est pas certain que la technologie Bluetooth puisse être utilisée aux fins sus-citées, d'autant plus qu'en excluant Google et Apple de l'interface, la détection des personnes ne sera possible que si l'application reste constamment ouverte sur notre téléphone et au premier plan.

Rappelons par ailleurs que l'option elle-même n'est pas sécurisée. Les experts en informatique recommandent en règle générale, de le désactiver. En effet, le Bluetooth est une porte d'entrée pour tous types de piratages et de traçage.

Avec cette technologie il est aisé de savoir qui a cette application ou qui ne l'a pas. Ainsi, l'accès à certains espaces publics, pourrait être subordonné à la détention de cette application.

Le fichage à grande échelle

Comme indiqué plus haut, il serait possible de réidentifier les pseudonymes, et donc de récupérer ces données pour constituer un fichage.

Les experts font état de la possibilité, à partir des informations de la base de données de Stop Covid, de créer une application améliorée qui permettrait de lui adosser un système de géolocalisation.

En outre, les données des individus pourraient être vendues à des assurances ou employeurs qui ne voudraient pas accorder services ou emploi à des personnes atteintes de la maladie et potentiellement porteuses de séquelles.

La cybercriminalité elle aussi entre en jeu, et pourrait créer des virus permettant de lancer une fausse alerte sur des téléphones à proximité pour voir certaines personnes choisies observer une quarantaine.

Si certaines de ces dérives peuvent paraitre moins dangereuses que d'autres, il convient donc de mettre chacune d'entre elles en perspective avec le risque sanitaire qui pèse sur notre société aujourd'hui.

III. LA NÉCÉSSITÉ DE CRÉER DES GARDE-FOUS POUR ÉVITER TOUTES FORMES DE DÉRIVES

Les précédents avertissements, nous invitent à nous questionner plus largement sur l'utilisation du numérique.

La gestion de cette crise sanitaire apporte une réponse sécuritaire couplée à un accroissement des pouvoirs gouvernementaux. On le voit aujourd'hui avec la création d'un état d'urgence sanitaire. Cette situation doit être limitée dans le temps par la législation. En outre, il est impératif de prévenir le risque d'une acceptabilité sociale de certaines dérives sous le prétexte de la crise.

A. L'ENCADREMENT LÉGISLATIF

La protection des données dans le cadre européen et national

L'Europe est attentive à la sécurité de nos données numériques et s'est équipée d'outils juridiques et structurels.

Ainsi, en 2018, elle met en œuvre dans tous les pays membres, le Règlement Général sur la Protection des Données (RGPD), document qui conforte la disposition déjà présente au sein de la Charte des Droits Fondamentaux de l'Union Européenne relative à la protection des données à caractère personnel, qui doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée. Le RGPD tient compte de l'utilisation massive des technologies ces dernières années et de la production d'un nombre incalculable de données l'accompagnant.

Les mécanismes de contrôle du règlement se déclinent au niveau national français avec la CNIL (Commission Nationale de l'Informatique et des Libertés), organe indépendant qui voit son rôle réaffirmé. Des représentants des autorités de protection des données des Etats membres composent le comité européen des protections de données (EDPB) qui s'assure que la loi est bien appliquée par tous les Etats membres.

Parmi les droits prévus pour les individus on trouve, entre autres, le droit de s'opposer à la récolte des données, le droit de faire supprimer ses données ou encore le droit d'information en cas de mise en péril ou d'atteinte aux données.

Malgré ces règles européennes, des dérogations sont prévues notamment dans le cadre de la protection de la santé des individus. [7]

L'avis de la CNIL sur le projet Stop Covid

La CNIL, sollicitée par le Secrétaire d'Etat au Numérique, a rendu, le 24 avril, un avis sur le projet Stop Covid. Elle demande certaines "garanties supplémentaires" et propose de donner un nouvel avis après le débat parlementaire prévu pour examiner le projet définitif de l'application.

Elle rappelle que la collecte des traces pseudonymes établissant une liste des personnes dont chaque porteur de l'application a été physiquement proche, "*pendant une durée circonscrite, parmi tous les porteurs de l'application (…) et qui a vocation à s'appliquer à la plus grande partie de la population possible, doit être envisagée avec une grande prudence*".

"*S'agissant du cas spécifique du traitement de données relatives à la santé des personnes concernées, le RGPD prévoit que le traitement de telles données peut notamment intervenir, comme en l'espèce, pour des motifs d'intérêt public « dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé », dès lors que ce traitement est nécessaire à ces fins et prévu par le droit de l'Union ou le droit national et que celui-ci prévoit « des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée » (article 9-2-i du RGPD). Sans préjudice de la possibilité juridique de fonder le traitement de ces données sur une autre exception prévue par l'article 9 du RGPD, la Commission estime que ces dispositions paraissent les plus adaptées à la situation de l'application StopCovid. Dans ces conditions, la Commission recommande que le recours à un dispositif volontaire de suivi de contact pour gérer la crise sanitaire actuelle dispose d'un fondement juridique explicite et précis dans le droit national.*"[8]

Si la CNIL salue les concepts d'anonymat et de volontariat, elle demande cependant des garanties supplémentaires.

Les garanties de sécurité qu'il nous semble impératif d'obtenir

- **S'assurer que l'application suive le but qui lui est bien attribué en rendant public son codage-source et ses possibles évolutions.**

La CNIL le rappelle : " *le principe de limitation des finalités, consacré par l'article 5(1) (b) du RGPD, est un principe cardinal de la protection des données à caractère personnel : celles-ci ne doivent être utilisées que pour un objectif précis et déterminé à l'avance. Toute autre utilisation des données est en principe interdite. (…) L'application StopCovid n'a pas pour objet de surveiller le respect de mesures de confinement ou d'autres obligations sanitaires.*"

En rendant public le codage-source de l'application et ses possibles évolutions, la société se dote d'un moyen de contrôle plus fort via la communauté informatique. Le Secrétaire d'Etat a annoncé qu'une partie du code source sera publiée le 12 mai pour permettre à tous les codeurs de vérifier le fonctionnement de cette application. Les premiers éléments rendus public ont provoqué l'agacement d'un certain nombre de développeurs, estimant qu'ils ne permettent ni d'opérer un réel contrôle pour l'heure, ni de faire remonter de nouvelles réflexions.

[7] Article 9 du RGPD.

[8] Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid », page 6

- **S'assurer que l'application ne sera pas la condition sine qua non pour accéder à des établissements publics ou privés, ni qu'elle sera utilisée pour sanctionner des comportements dérogatoires aux recommandations sanitaires**

Il ne faudrait pas que cette application, à l'origine basée sur le volontariat, se transforme en un passeport obligatoire notamment pour accéder à certains lieux et espaces, à l'instar de ce qu'il s'est passé Singapour.

Surtout, qu'il ne s'accompagne pas de sanctions, cela n'étant pas prévu lors de la création de l'application.

Là encore, la CNIL rappelle : "*L'utilisation d'une application sur la base du volontariat ne devrait pas conditionner ni la possibilité de se déplacer, dans le cadre de la levée du confinement, ni l'accès à certains services, tels que par exemple les transports en commun. Les utilisateurs de l'application ne devraient pas davantage être contraints de sortir en possession de leurs équipements mobiles. Les institutions publiques ou les employeurs ou toute autre personne ne devraient pas subordonner certains droits ou accès à l'utilisation de cette application. Ceci constituerait en outre, en l'état du droit et selon l'analyse de la Commission, une discrimination.*".

- **S'assurer du caractère éphémère de la liste de données**

Les données, même anonymes, doivent pouvoir être effacées régulièrement des listes de malades ou cas-contacts.

"*le respect du principe de proportionnalité se traduira notamment par une collecte et une conservation des données limitées à ce qui est strictement nécessaire, afin de minimiser l'atteinte portée à la vie privée des personnes. Cette garantie fondamentale implique en l'espèce que la collecte et le traitement de données opérés par l'application revêtent un caractère temporaire, d'une durée limitée à celle de l'utilité du dispositif au regard des finalités précédemment décrites. Elle implique également que toutes les données soient supprimées dès le moment où l'utilité de l'application ne sera plus avérée. Dans l'hypothèse où une exploitation statistique ou à des fins de recherche scientifique se révélerait néanmoins nécessaire, celle-ci devra être réalisée en priorité sur des données anonymisées ou, à défaut, dans le strict respect des règles fixées par le RGPD et la loi « Informatique et Libertés »*[9].

- **S'assurer de son encadrement dans le temps**

Il convient de veiller à ce que les outils limitateurs de libertés, censés être provisoires le temps de la crise, ne soient pas transformés en dispositifs permanents et obligatoires. Si la mise en place d'une application de tracing se justifie aujourd'hui et est mise en place sous l'état d'urgence sanitaire, lui-même instauré par une procédure accélérée, qu'en sera-t-il demain lorsque l'état d'exception sera levé ?

Selon la Quadrature du Net, association de défense des droits et libertés sur internet, ces demandes de garanties sont vaines. Le collectif estime que la CNIL, via cet avis, n'a pas tenu son rôle. Il rappelle qu'à ce jour, aucune étude ni aucun élément ne prouve l'efficacité de cette technique qui selon lui, porte atteinte aux libertés fondamentales et qu'en ce sens, la CNIL devrait rendre un avis, à ce jour, non conforme. D'autre part il soutient que les conditions pour obtenir une application

[9] Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid », page 7.

respectueuse des libertés sont impossibles à remplir : l'anonymat est impossible, tout comme le consentement libre en période de crise. [10]

B. L'ACCEPTABILITÉ SOCIALE DE CERTAINES DÉRIVES SOUS LE PRÉTEXTE DE LA CRISE

Les enseignements du passé

Pour protéger nos libertés, la loi est aussi indispensable que la vigilance de la population sur les dérives liées à l'utilisation des nouvelles technologies. Cette prise de conscience est d'autant plus difficile qu'elle se déroule actuellement dans un contexte de peur et d'urgence imposé par la crise sanitaire. Un exemple significatif et d'actualité : l'extension à un plus grand nombre de départements de l'expérimentation des Cours criminelles sans jurés populaires, au prétexte de la crise, est dénoncée par de nombreux juristes comme l'effacement définitif de la Cour d'Assises au profit d'une justice au rabais. Il est donc impératif de mener une réflexion plus globale sur la façon dont le progrès peut nous être présenté et ses possibles dérives à moyen ou long terme.

D'autant qu'il existe en droit français, des précédents de dispositifs, justifiés dans leur principe, qui ont été dévoyés par la suite. A titre d'exemple, la généralisation du fichage ADN a été opérée en droit français en 2003. Le FNAEG (Fichier National Automatisé des Empreintes Génétiques), a été créé en 1998, à la suite de l'arrestation du tueur en série parisien Guy Georges. Destiné à l'origine aux infractions sexuelles, ce fichier a été étendu à partir de 2003 à la quasi-totalité des crimes et délits, à l'exception notamment des délits financiers. Les personnes simplement mises en cause dans une affaire, bien que non encore condamnée, sont visées par le dispositif. Quant au refus de prélèvement, la loi en a fait un délit. En effet, l'article 706-56 du Code de procédure pénale précise que "le fait de refuser de se soumettre au prélèvement biologique ... est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Lorsque ces faits sont commis par une personne condamnée pour crime, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende". Enfin les données génétiques sont conservées pendant quarante ans pour les personnes condamnées et vingt-cinq ans pour les autres.

En 2018, selon la CNIL, 2,9 millions de profils génétiques étaient ainsi inscrits dans le FNAEG[11].

La tendance actuelle de l'utilisation de la technologie pour assurer la sécurité

La ville de Nice, après l'attentat de 2016 sur la Promenade des Anglais, a voté un plan d'expérimentations notamment sur la reconnaissance faciale, l'utilisation de caméras pour détecter les émotions dans les transports, ou des applications de vigilance citoyennes. Pour justifier ces choix, Christian Estrosi rappelle que la France est en guerre, "*s'interdire d'utiliser un moyen qui pourrait épargner des vies, qui pourrait épargner des conséquences graves pour notre pays et sa sécurité serait porter une lourde*

[10] *"LA CNIL S'ARRÊTE À MI-CHEMIN CONTRE STOPCOVID", 27 avril 2020 (https://www.laquadrature.net/2020/04/27/la-cnil-sarrete-a-mi-chemin-contre-stopcovid/).*

[11] Observons que depuis des années, les juristes corses ont été en première ligne dans le combat contre les dérives liées au fichage ADN. Sur la « jurisprudence corse », voir notamment : F.-B. Huyghe, ADN et enquêtes criminelles, PUF, 2008, p. 93.

responsabilité (…). La guerre du 21ème siècle se mène avec les armes du 21ème siècle."[12] Si aujourd'hui, le système de reconnaissance faciale est interdit en France, la ville de Nice souhaite ouvrir une réflexion commune sur l'opportunité de ces moyens.

Aujourd'hui, la notion de "Safe City" est souvent mise en avant, en particulier depuis les événements meurtriers qui nous ont touchés dans un passé récent. Le terrorisme a justifié et justifie encore, toutes les mesures qui placent la sécurité au premier rang des décisions politiques jusqu'à l'utilisation des technologies visant à la surveillance de masse.

La technologie nous est souvent présentée comme une réponse à un problème social donné. Certains dénoncent cependant, un "solutionnisme", c'est à dire la tendance à "*laisser les causes d'un problème inchangé tout en se concentrant sur la tâche plus abordable consistant à « ajuster » le comportement individuel à l'inaltérable réalité, aussi cruelle soit-elle.*"[13]

Cette notion d'ajustement laisse la part belle à la technologie. Combinée à la peur dans un contexte de pandémie, elle contribue elle aussi, à faire accepter de façon consensuelle, le recours à des instruments de surveillance. On peut alors glisser vers un changement de culture, de regard, et concevoir comme une évidence le fait de contrôler toujours davantage.

Dans son avis, la CNIL rappelle que "*le recours à des formes inédites de traitement de données peut en outre créer dans la population un phénomène d'accoutumance propre à dégrader le niveau de protection de la vie privée* "[14].

L'exemple de la Chine

Le modèle chinois est un cas d'école. Il montre l'instauration d'une véritable dictature numérique, acceptée par une large tranche de la population, habituée à toutes formes de contrôles depuis les débuts de la République Populaire communiste. Aujourd'hui, dans certaines villes chinoises, les habitants se soumettent à l'instauration d'un "crédit social". On peut résumer ce concept par un système de notation distinguant en plusieurs catégories les bons citoyens des mauvais, c'est-à-dire ceux qui suivent les règles édictées par le parti et ceux qui ne les suivent pas.

À la clé de cette notation : l'accès ou non à des biens et services tels que la possibilité de voyager ou encore l'obtention de prêts bancaires, ou d'un logement.

À son origine : la collecte très importante de données numériques (recherches internet, données de police, données administratives…), combinée à un réseau extrêmement dense de caméras dotées d'un système de reconnaissance faciale. Le pays en possédait déjà 170 millions en 2019.

Or, en Chine, cette pratique est acceptée, l'intérêt du groupe devant primer sur l'intérêt individuel, quitte à perdre la possibilité de sortir du rang. Cela ne va pas sans rappeler un monde dystopique déjà décrit par la littérature, où la principale réussite d'un gouvernement est de faire croire à sa population que le modèle de société institué et totalitaire est bien celui voulu par les individus qui s'en satisfont. (cf, par exemple, "Le Meilleur des Mondes", d'Aldous Huxley).

[12] Interview dans "*Tous surveillés : 7 milliards de suspects*", documentaire de Sylvain Louvet.
[13] "*Covid-19, le solutionnisme n'est pas la solution*", Le Monde Diplomatique, 5 avril 2020.
[14] Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid », page 3.

La Chine souhaiterait exporter son modèle et parle de "nouvelles routes de la soie numérique". Ainsi, 60 à 80 pays pourraient être intéressés par les technologies de surveillance chinoises, dont la France, sans qu'il soit évidemment question, pour l'heure, d'en faire une application aussi systématique.

Certaines facilités à accepter l'utilisation de technologies pourraient laisser craindre que la société européenne devienne un jour assez mûre pour recevoir une culture numérique totalitaire.

L'évolution de la perception des outils numériques dans notre société

On voit en effet, toutes proportions gardées, s'installer peu à peu en Europe le même fil de pensée, sans réaliser que l'on pourrait créer progressivement une société paranoïaque, faite de suspects, d'individus potentiellement dangereux pour l'Autre...

Un sondage auprès de 1000 Français, commandé par l'Université d'Oxford et portant sur une application similaire à Stop Covid[15], montre que 48% des interrogés souhaiterait l'installer *« sans aucun doute »*, 31 % le feront "*probablement " et "près de deux personnes interrogées sur trois seraient favorables à ce que cette application soit installée automatiquement par les opérateurs téléphoniques*". Enfin, seul un quart des sondés se méfie des risques de piratage et de la possibilité pour cette application de s'inscrire plus durablement dans le temps.

S'il n'est pas raisonnable de tirer des enseignements généraux de ces résultats, étant donné le peu d'informations détenues par les sondés et que "*le sondage prend comme acquis que l'application est parfaitement fonctionnelle, sans bug, et permettra effectivement de contribuer à la lutte contre la pandémie*", ces chiffres restent inquiétants quant au peu de méfiance dont font preuve les personnes interrogées. L'absence de méfiance envers des outils numériques qui ne sont contrôlés que par une minorité de sachants, les entreprises ou les gouvernements, peut s'expliquer par le manque de connaissances sur les dérives possibles. Paradoxalement, la peur irraisonnée, en l'occurrence du virus, se nourrit également du caractère lacunaire de nos connaissances à son sujet. C'est pourquoi la vulgarisation apparait comme essentielle, s'agissant de ces questions, tant il est vrai qu'elles sont encore insuffisamment partagées par le plus grand nombre.

Il est important d'être attentif à l'inclination de nos systèmes à s'ouvrir à des méthodes liberticides déjà appliquées dans d'autres pays. Il est donc nécessaire de demeurer parfaitement attentifs aux alertes s'agissant des atteintes à nos libertés individuelles, notamment en assurant un large espace d'intervention à ceux qui entendent les dénoncer, comme certains professionnels du numérique, les barreaux ou les associations de défense des droits de l'Homme.

Leur rôle pourrait également être de mener un travail de pédagogie et de vulgarisation sur ce qui est présenté comme un progrès mais qui pourrait rapidement devenir un instrument d'oppression dans le futur.

Parce que notre liberté ne doit pas être sacrifiée par peur ou par méconnaissance, il est d'ores et déjà nécessaire de nous positionner collectivement sur ces questions, comme l'ont fait par exemple

[15] "*Acceptabilité d'une application téléphone pour tracer les contacts porteurs du Covid-19*", 6 avril 2020.

certaines villes américaines (San Francisco, Oakland...) qui ont exclu l'utilisation de caméras à reconnaissance faciale.

CONCLUSION

L'urgence de la crise ne doit pas nous dispenser de nous poser des questions sur l'utilisation de nouvelles technologies. Les conditions d'efficacité d'une application telle que Stop Covid sont encore nombreuses à mettre en place, et les garanties de sécurité sont, pour l'heure, non fournies. Si des contrôles existent d'ores et déjà, il est légitime de participer au débat sur le juste équilibre à trouver entre la sécurité et la liberté.

S'il est vrai que les outils numériques peuvent apporter de nombreux bénéfices à la lutte contre l'épidémie actuelle, ce qui peut sembler légitime aujourd'hui doit pouvoir être remis en débat demain.

C'est la raison pour laquelle, une partie de la communauté du numérique, qui rappelle que "*un principe essentiel en sécurité informatique est que l'innocuité d'un système ne doit en aucun cas être présumée en comptant sur l'honnêteté de certains de ses acteurs*"[16], devrait pouvoir bénéficier d'une oreille attentive de la part de nos institutions, sur les projets de création d'instruments informatiques pouvant menacer la bonne utilisation de nos données personnelles.

De cette façon, les autorités publiques - sous l'éclairage d'un large et permanent débat au sein de l'espace public pourront se positionner en conscience sur ces sujets d'actualité primordiaux.

[16] "Le traçage anonyme, dangereux oxymore - Analyse de risques à destination des non spécialistes", 21 avril 2020.