Publié le 7 mai 2020

Stopcovid et stop libertés

Les Français se réveilleront-ils demain surveillés par des mouchards numériques ? En Asie, des populations entières le sont déjà. La France des Lumières et de l'individualisme-roi va-t-elle l'accepter aussi facilement que les pays asiatiques ? La peur de la contagion risque d'être mauvaise conseillère. Un regard dépassionné sur une question aussi techniquement complexe que grave du point de vue éthique et politique n'a rien d'évident par les temps qui courent.

Une société stressée est une société manipulable. Or, après deux mois de confinement, la peur, la colère sont au rendez-vous. La distanciation sociale et internet ne changent pas les mécanismes de la psychologie humaine. Gustave Le Bon, dans un ouvrage resté célèbre, *La psychologie des foules*, paru en 1895, l'avait d'ailleurs anticipé : «Des milliers d'individus séparés peuvent à certains moments, sous l'influence de certaines émotions violentes, un grand événement national par exemple, acquérir les caractères d'une foule psychologique[1]» Nous y sommes. Sa théorie de la contagion sociale qui rend les individus «suggestibles» et «irresponsables» semble même avoir gagné en actualité avec les réseaux sociaux.

Le doigt dans un engrenage liberticide

Dans ce contexte où l'angoisse est palpable, le Gouvernement français et les mandarins qui le conseillent projettent de mettre en place à grande échelle un outil de surveillance des faits et gestes de la population : le StopCovid. Selon un sondage Odoxa, 62 % de la population, terrorisée par les risques liés à la propagation d'un virus à fort taux de létalité, serait prêt à télécharger un tel système de surveillance. Même Gaspar Koenig, président du *think tank* «Génération libre», ancien collaborateur de Christine Lagarde et grand défenseur de l'anonymat, soutient l'idée et dénonce l'égoïsme de ceux qui s'y opposent. Conditionnés par la peur de la contagion, les Français sont prêts dans la foulée à accepter l'installation de caméras thermiques (79 %) et ne seraient pas contre la généralisation des systèmes de reconnaissance faciale tels que ceux d'ores et déjà expérimentés à Nice (51 %).

Les raisons invoquées sont bien entendu louables. Puisque les GAFA utilisent largement nos données privées pour nous vendre des biens et des services pas toujours indispensables, pourquoi ne pas utiliser ces données qui transitent via leurs réseaux pour lutter contre la pandémie ? L'objectif sanitaire affiché n'est pas discutable. Qui ne voudrait pas tout faire pour éviter que la maladie ne fasse davantage de morts ?

1 - Gustave Le Bon, *La psychologie des foules*, Alcan, 1895 (rééd. PUF 2013), chapitre 1.

Mais à quel prix ? Jusqu'à accepter la mise en place d'une véritable «dictature sanitaire[2]» ? Au nom de la santé publique, un État peut-il violer l'intimité de ses concitoyens ? Est-il acceptable que l'État, même en période de pandémie, utilise des informations qui relèvent de la vie privée, en principe confidentielles, et restreigne drastiquement des libertés aussi fondamentales que le droit de circuler librement sur l'ensemble du territoire ?

Cet outil de contrôle de nos vies personnelles, qui sera vraisemblablement plébiscité pour de «bonnes» raisons, peut s'avérer un terrible piège s'il tombe, demain, aux mains de gouvernements peu respectueux des libertés publiques. Si le confinement généralisé et obligatoire pose déjà un problème éthique, qu'en sera-t-il d'un confinement sélectif qui se ferait sur la base d'informations recueillies à l'insu des personnes ?

Les défenseurs du projet StopCovid affirment que cette application a un temps de vie limité et qu'il y sera mis fin avec l'éradication du Coronavirus, que la diffusion des données et l'anonymat des personnes contacts seront protégés, et que cela se fera sur le mode du volontariat. Mais qui peut l'affirmer si les données sont massivement centralisées ?

Malheureusement, les promesses dans ce domaine sont rarement tenues. On peut légitimement s'interroger sur le choix qui a été fait en 2017 de déployer sur tout le territoire le fichier TES qui recense l'ensemble de la population française dans une méga-base regroupant nos données biométriques dans le but affiché de lutter contre la production de faux titres d'identité.

Utiliser des outils de suivi numérique de la population revient à mettre le doigt dans un engrenage qui peut, à terme, s'avérer liberticide et devenir un instrument de contrôle très puissant de la population, comme c'est déjà le cas en Chine.

Enfin, et ce n'est pas la moindre des questions, les contraintes techniques sont loin d'être résolues et la solution que la France tente de valider n'est pas la mieux placée face à l'alliance Apple/Google qui, paradoxalement du point de vue du respect de la «*privacy by design*», présente plus de garanties que la solution tricolore qui tient à remonter toutes les informations recueillies vers un serveur central…

Taiwan et le modèle asiatique

Cette idée de tracer les malades ou les personnes à risque vient, comme le virus, de Chine, de Taïwan exactement. À 130 km des côtes chinoises, l'île est le pays le plus exposé à l'épidémie. Dès le mois de décembre 2019, elle alerte l'OMS, dont elle est exclue à la demande de Pékin.

Taïwan, qui a déjà payé un lourd tribut à l'épidémie du SRAS (2002-2003), ne fait pas confiance aux Chinois du continent. Tous les vols provenant de Chine sont immédiatement surveillés. La température des passagers est prise à la descente de l'avion. Ceux qui présentent des signes d'infection sont assignés à résidence chez eux. Leurs déplacements sont suivis grâce au signal GPS de leur téléphone portable et appelés régulièrement pour surveiller qu'ils ne s'éloignent pas de celui-ci. Un «chatbot» (petit programme qui «dialogue» à partir de mots clés avec un utilisateur),

2 - Jean-Yves LE GALLOU in Polemia, avril 2020.

leur envoie des alertes pour leur rappeler de prendre leur température ou les invite à poser des questions à l'équipe de suivi médical.

Grâce à ce «*tracking*», les autorités sanitaires taïwanaises ont rapidement dressé une carte détaillée de tous ceux qui avaient contracté le Covid-19. Ils ont intégré ces données personnelles (déplacements, consultations, symptômes, antécédents, etc.) dans l'équivalent taïwanais de leur carte vitale et dans le fichier des douanes qu'ils ont interconnecté. Ainsi, le 31 janvier 2020, après la confirmation qu'un passager du navire de croisière *Diamond Princess* avait été testé positif au Covid-19, tous les passagers ayant débarqué dans le port de Keelung et tous les points où ils étaient passés ont été communiqués par SMS aux taïwanais, leur conseillant vivement de se mettre en quarantaine au cas où ils auraient pu croiser les lieux traversés par les passagers du navire[3]. Taïwan a ainsi été capable de tracer chez elle la quasi-totalité de la chaîne de contamination. Elle a même annoncé à la France son premier cas : un médecin français qui avait examiné une guide touristique sans porter de masque…

Le dispositif a été complété par un traitement de vidéosurveillance susceptible d'estimer la proportion de personnes masquées. Quant aux données obtenues, elles ont été mises à disposition du public en libre accès. De nombreux développeurs privés se sont rués sur ce programme «*open source*» pour proposer des applications diverses et variées, comme des assistants vocaux, des moteurs de recherche permettant, par exemple, de connaître en temps réel le stock des masques en pharmacie. Tous les hôpitaux, cliniques et pharmacies ont ainsi eu les informations de chaque «patient». Quant aux mesures de quarantaine, elles ont été appliquées sous la menace d'amendes pouvant monter jusqu'à 33 000 dollars !

Résultat : Taïwan a endigué l'épidémie et, à ce jour, l'île de 24 millions d'habitants compte moins de dix décès du Covid-19. Un score qui, évidemment, donne envie, à condition d'être applicable.

La Corée du Sud n'est pas en reste. Depuis l'épidémie du SRAS, le Gouvernement s'est octroyé un droit total d'accès aux données personnelles. Il va en faire un large usage. Comme à Taïwan, ces données rendues publiques ont été réutilisées par diverses applications. Ainsi, les déplacements des malades sont reconstitués au travers des images de vidéosurveillance, l'utilisation de leur carte bancaire ou le GPS de leur smartphone. Dès qu'un nouveau cas est détecté, un SMS est envoyé à ceux, voisins ou collègues de travail, qui auraient été susceptibles de le croiser. Le succès de ces mesures, couplées avec un dépistage massif, s'est révélé moins performant qu'à Taïwan, mais bien meilleur que dans beaucoup d'autres pays.

Autre exemple asiatique : Hong Kong, où un bracelet est remis à chaque personne parvenant sur le territoire, couplé à une application à télécharger sur son téléphone.

Singapour aussi possède son système de traçage numérique «*TraceTogether*», proche de ce qui pourrait être développé chez nous. Basé sur la technologie Bluetooth, il permet de détecter la proximité du smartphone d'une personne infectée et d'enregistrer ses contacts, qui sont automatiquement alertés sur une possible contamination. L'utilisation de l'application est libre.

3 - Voir L'Usine Nouvelle.

Conséquence : moins de 20 % de la population l'utilise. La méthode a échoué, et Singapour a dû être confinée.

L'archétype chinois

Reste le cas de la Chine. C'est à elle que l'on doit l'épidémie et le système de contrôle de la population le plus élaboré. Il a été pleinement utilisé contre la pandémie.

C'est sur la base d'informations qui sont centralisées dans des bases de données numériques que le confinement des proches d'un contaminé est décidé en Chine. Le traçage ne s'arrête pas là. Un QR code (code barre à deux dimensions) changeant de couleur (vert ou rouge) en fonction du risque contagieux est affecté à chaque Chinois. Calculé selon des algorithmes qui sont tout sauf transparents, il prend en compte les contacts, les déplacements, mais aussi l'historique des paramètres de santé. Selon que le QR code est rouge ou vert, l'accès est ou non possible aux transports, magasins, résidences ou services publics. Le système est couplé à celui de la reconnaissance faciale, qui s'appuie sur 300 millions de caméras de vidéosurveillance et des capteurs thermiques disposés dans les lieux d'infection. Ces caméras et ces capteurs permettent aux autorités de détecter tout suspect et de surveiller le comportement des citoyens, par exemple le port du masque.

Centralisées au niveau national, ces informations permettent d'alimenter le système de notation sociale de la population. Chaque citoyen, doté de 100 points, se voit ainsi attribuer par les autorités des bonus ou des malus en fonction de son comportement, avec évidemment des conséquences, agréables ou désagréables, pour sa vie quotidienne.

Le Parti communiste chinois a ainsi mis en place un système de délation numérique, parfaitement anonyme, et qui fonctionne en temps réel, sans pour autant renoncer aux classiques comités de quartier, aux mouchards sur les portes et aux traditionnels micros installés dans les maisons. Le pays est ainsi couvert de millions de cellules et autres capteurs. Un maillage étroit de tous les lieux de vie permet aux commissaires politiques de s'assurer facilement du bon respect de la quarantaine.

Plus proche de nous, Israël n'est pas très loin de la Chine dans la surveillance de sa population. Ce sont les Services de Sécurité intérieure (Shin-Beth) familiers de l'antiterrorisme qui sont chargés de la lutte contre l'épidémie. Tel-Aviv utilise ainsi massivement les données privées via les applications téléphoniques, mais aussi des drones et tous les moyens du contre-espionnage, avec un réel succès d'ailleurs.

L'Europe acquise au «*tracking*»

En Europe, nous sommes loin de ces excès. Pour autant, la méthode asiatique, tout comme le virus, gagne du terrain. La Pologne impose à toute personne suspecte 14 jours de confinement strict. Pour en assurer le contrôle, elle propose au «suspect» soit une application lui permettant de se prendre régulièrement en «selfie» avec son téléphone, soit d'accepter plusieurs fois par jour le passage des forces de l'ordre à son domicile. La Pologne a par ailleurs en projet une application dite «Protego», qui utiliserait la technologie Bluetooth sur une plateforme Apple-Google en cours de développement.

L'Allemagne utilise depuis peu les données d'un bracelet connecté pour cartographier la progression du virus. Elle prépare une application «Corona-Datenspende», qui devrait être utilisée sur la base du volontariat et permettrait de recueillir des données comme l'augmentation du pouls au repos, les modifications dans les habitudes de sommeil et d'activités, la taille, le poids ainsi que des éléments comme le code postal. Ces «*data*» recueillies par l'Institut de santé Robert Koch de manière anonyme sont destinées à être utilisées exclusivement à des fins statistiques, est-il précisé par les autorités sanitaires. Les résultats seront publiés sur une carte interactive. Les initiateurs du projet espèrent 100 000 chargements de l'application.

Quand on fait le bilan de ces expériences d'utilisation de «*tracking*» numérique de l'épidémie, force est de constater qu'en dehors des pays les plus totalitaires, l'effet sur la propagation de l'épidémie est loin d'être probant. Quelles conclusions en tirer pour la France ?

Le StopCovid français

En France, une application est en cours de développement : le StopCovid. Elle est basée, comme à Singapour, sur l'utilisation de la technologie Bluetooth. Son utilisation n'aurait aucun caractère obligatoire et permettrait à celui qui l'aurait téléchargée d'être alerté d'un risque de contagion à la suite d'un «contact» avec un porteur du virus.

Pour le moment, plusieurs problèmes à la fois techniques et politiques non résolus contrarient son développement.

En effet, pour être performant, le tracking doit couvrir selon certains spécialistes au moins 70 % de la population. Parvenir à ce taux n'a rien d'évident. En France, 10 % de la population habite dans une zone non couverte par les réseaux téléphoniques, 25 % de la population n'a pas de téléphone portable, 62 % de ceux qui en possèdent seraient prêts à charger l'application. Dans ces conditions, à peine un Français sur deux pourrait être «surveillé». Insuffisant pour être efficace.

À cette première contrainte s'en ajoute une autre, de taille. Une application de signalement téléphonique ne peut être utile que si le dépistage du virus est massif dans la population. Concevoir une application pour signaler que l'on a approché ou croisé un porteur du virus, si celui-ci n'a pas été préalablement diagnostiqué, ne sert pas à grand-chose !

En dépit de cette contrainte, l'INRIA (l'Institut national de recherche pour les sciences et technologies du numérique) développe, en partenariat avec des partenaires allemands et français – notamment le CNRS, des grandes écoles, l'INSERM et d'autres centres de recherche – un protocole appelé ROBERT (ROBust and privacy-presERving proximity Tracing), conforme à la législation européenne sur la protection des données (RGPD).

À proprement parler, il ne s'agit pas d'une application de *tracking* des individus, car elle n'utilise que le Bluetooth et aucune donnée de bornage GSM ou de géolocalisation. Elle ne fait donc que signaler la proximité de deux téléphones. Son principe est le même que celui des enquêtes de terrain conduites traditionnellement par les services médicaux pour tracer les épidémies. Voici ce qu'en dit le Président de l'INRIA, Bruno Sportisse : «Une telle application n'est pas une application de surveillance : elle est totalement anonyme. Pour être encore plus clair : sa conception permet que

PERSONNE, pas même l'État, n'ait accès à la liste des personnes diagnostiquées positives ou à la liste des interactions sociales entre les personnes. La seule information qui m'est notifiée est que mon *smartphone* s'est trouvé dans les jours précédents à proximité du *smartphone* d'au moins une personne qui a, depuis, été testée positive et s'est déclarée dans l'application.»

Le protocole ne communique que ce que l'on appelle des «crypto-identifiants», qui ne permettent pas d'identifier les personnes. Comme le déclare encore Bruno Sportisse : «Une telle application n'est pas une application de délation : dans le cas où je suis notifié, je ne sais pas qui est à l'origine de la notification. Lorsque c'est moi qui me déclare positif, je ne sais pas qui est notifié. Une telle application n'est pas obligatoire. Ses utilisateurs choisissent de l'installer. Ils choisissent d'activer le Bluetooth. Ils peuvent, à tout moment, désactiver le Bluetooth ou désinstaller l'application.»

De leur côté, Apple et Google se sont mis d'accord pour développer une API, c'est-à-dire un jeu de commande qui permettrait d'utiliser le Bluetooth des appareils dans la configuration de leurs deux systèmes d'exploitation. Ce jeu de commande laisserait aux États la possibilité de gérer à leur guise l'infrastructure technique associée à l'application, tout en conservant la souveraineté sur l'usage des données. Le malheur veut que le système que développe Apple/Goggle soit actuellement incompatible avec les normes européennes et le protocole ROBERT. En outre, la solution franco-européenne ne peut pas se passer d'un accord technique avec Apple et Google pour permettre en particulier d'utiliser les fonctionnalités du Bluetooth en mode de veille. Dans ces conditions, le bras de fer est inévitable, et un accord rapide entre les Américains et la France apparaît peu probable. Faut-il s'en réjouir ou le déplorer ?

À quelles conditions ?

Pour qu'une solution de «*tracking*» soit efficace sans être liberticide, il faudrait en premier lieu être assuré que la population joue le jeu. Les Français ne sont pas chinois, mais gaulois. Aujourd'hui, quand on leur pose la question, ils semblent d'accord pour l'utiliser. Mais demain ? Resteront-ils assez motivés et disciplinés pour la mettre en pratique durablement et ne pas oublier de s'en servir ? Il faudrait notamment que les problèmes fonctionnels pénalisants liés à l'usage du Bluetooth soient réglés. Actuellement, la version IOS d'Apple ne fonctionne pas en tâche de fond. Quant à la version Android, elle est lourdement consommatrice d'énergie et ne permet pas simultanément l'emploi d'un casque Bluetooth. Ces inconvénients pourraient en décourager certains.

Pour qu'ils acceptent massivement cette surveillance, il faudrait encore que les Français soient rassurés sur la confidentialité du système. Cela suppose que le système soit sous le contrôle d'un opérateur indépendant qui ne soit ni un État, ni une société privée. La CNIL – ou l'EDPB, son équivalent européen – semblent tout indiqués. Les deux organismes ont fait leurs preuves en matière de protection des données. L'anonymat doit en effet être la règle d'or. Il ne devrait exister aucun fichier centralisé, aucune donnée privée ou liste de contacts exportée, et les données cryptées et transmises devraient l'être de manière automatique, sans possibilité d'intervention humaine selon une technologie dite «*blockchain*». À ce prix, la technologie Bluetooth pourrait être complétée par des informations plus précises de géolocalisation, et un QR code pourrait être utilisé sans risque. Enfin, et cela ne dépend pas de la technologie numérique retenue, il faudrait que la population puisse être massivement testée. Nous n'en sommes pas là !

Singapour est souvent cité en exemple. Le Président de l'INRIA n'a pas manqué de rappeler que la solution française est proche de la solution utilisée dans la ville-État : transparence et sécurité des sources grâce au partage de l'application en *open source*, volontariat et respect absolu de l'anonymat. Mais, bien que Singapour soit une île de seulement 6 millions d'habitants, beaucoup plus technophile que la population française et plus «encadrée» socialement, le système n'a pas fonctionné et le Gouvernement a du décider un confinement total.

Dans ces conditions, les outils de *tracking* sont-ils nécessaires ? Les masques et le dépistage sont des moyens de lutte contre la pandémie que personne ne discute. Efficaces ou non, ils ne font courir aucun risque à leurs usagers. Les outils de *tracking* et de contrôle social sont d'une tout autre nature. Même maîtrisés, ils constituent potentiellement une menace pour les libertés. Pierre Manent déclarait récemment dans *Le Figaro* : «Personne ne conteste que la pandémie constitue une urgence et qu'avec l'urgence certaines mesures inhabituelles s'imposent. Mais la fragilité de la santé humaine constitue en quelque sorte une urgence permanente qui peut fournir à l'État une justification permanente pour un état d'exception permanent. Nous ne voyons plus dans l'État que le protecteur de nos droits ; dès lors, la vie étant le premier de nos droits, un boulevard est ouvert à l'inquisition de l'État.»

Lorsque la vie va reprendre un cours un peu plus normal, le risque sera en effet de présenter la victoire contre le Coronavirus acquise au moyen de mesures draconiennes et de l'utilisation quasi orwellienne de logiciels d'intelligence artificielle comme un nouveau modèle d'organisation sociale. Une question restera alors posée : sans la liberté, à quoi sert la santé ?

Thierry Boutet

Retrouvez cet article sur srp-presse.fr