Pourquoi je ne téléchargerai pas l’application StopCovid

Temps de lecture : minute

26 avril 2020

Depuis une dizaine de jours résonne une musique de plus en plus persistante autour des réflexions du gouvernement sur l’utilisation d’une application de tracking de la population pour lutter contre la propagation du coronavirus. Comme souvent avec les politiques, un “non” s’est transformé en “oui peut être” à la faveur d’un plan de communication destiné à préparer la population à une atteinte réelle de ses libertés fondamentales sous couvert d’état d’urgence sanitaire.

C’est l’histoire d’une vessie que l’on fait passer pour une lanterne

J’ai, depuis l’adolescence, pris l’habitude chaque matin en buvant mon café, de lire la presse nationale et internationale. Force est de constater que plus les années passent et plus ma tension artérielle monte au petit déjeuner. Loin de moi l’idée de prendre pour argent comptant les gros titres des journaux, mais cela me permet d’avoir une idée de la température quotidienne du monde. Depuis le week-end dernier centré autour de l’allocution présidentielle, c’est au tour de la société civile de n’avoir qu’un mot à la bouche : StopCovid.

Le moins que l’on puisse dire est que le débat est passionné et cela ne fait que commencer. L’hystérisation de la société est tout à fait normale

en cette période de grand stress. Les sentiments qui nous animent tels la peur et la colère sont cependant de très mauvais conseillers. Il me paraît très dangereux de laisser nos émotions dicter des choix pouvant s'avérer fortement impactant pour la population sur du long terme, sans s'interroger sur la pertinence des options retenues.

Simplicité, usage, efficacité et pragmatisme doivent être les maîtres mots de l'action publique sans aucun compromis sur nos valeurs. La technologie peut être d'une grande aide pour lutter contre la pandémie que nous vivons. Mais telle une arme dans cette guerre qui s'annonce longue, celle-ci ne peut être l'outil d'un repli sur soi, d'une peur de l'autre ou d'une perte d'espoir dans l'avenir par asservissement de l'humain.

Stigmatiser et moraliser n'est d'aucune aide

Chacun son métier. Nos choix définissent ce que nous sommes. Le discours de la lutte à tout prix n'est pas justifiable. Que des mandarins entourant le gouvernement s'expriment sur l'application StopCovid alors qu'ils ne sont déjà pas d'accord entre eux sur les traitements à préconiser pour guérir nos malades fait froid dans le dos. Que, Gaspard Konig, président du think tank Generation Libre et pour qui j'ai par ailleurs un grand respect, émette un vibrant appel en faveur de l'utilisation des données personnelles pour combattre la propagation de la pandémie me laisse sans voix.

Pourtant militant reconnu du droit à l'anonymat, le voici devenu promoteur de la stratégie gouvernementale. Allant jusqu'à dénoncer "l'insouciance égoïste de la génération Y", sous prétexte qu'elle utilise massivement déjà les applications des GAFAM hautement consommatrices de données privées, il dénonce leur refus de participer par tous les moyens à la lutte contre la propagation du virus sans se

poser initialement les bonnes questions. Stigmatiser et moraliser n’est d’aucune aide et ne conduit qu’à démultiplier les rancoeurs et l'irrationnel.

Non tous les moyens ne sont pas bons ! Je suis issu de la génération Y. Je suis, comme beaucoup, touché en mon sang par les conséquences sanitaires de cette pandémie. Il est normal de s'interroger, de mettre en doute l’information et de participer à l’élaboration d’une solution optimale pour tous. Le contraire serait criminel ! Plus que jamais nous avons besoin des autres sans oublier qui nous sommes. Notre histoire et nos valeurs sont le terreau sur lequel nous devons bâtir le futur. Ce serait une insulte faite à nos malades et nos morts de laisser faire n’importe quoi, de renier les fondamentaux de notre société, d’oublier que nous sommes la nation des droits de l’Homme ! Liberté, égalité, fraternité ne sont pas que des mots.

Prenons la hauteur nécessaire pour dépassionner les débats et regardons simplement les faits, sans moralisation, ni dogmatisme, ni passion.

Petit tour du monde des pratiques de tracking social

Taïwan

Par sa proximité et son histoire compliquée avec la Chine, Taïwan a dès la fin décembre 2019 pris les mesures adéquates et alerté en vain l’OMS sur la dangerosité du virus. Forte de son expérience douloureuse lors de la pandémie du SRAS et ne donnant aucun crédit aux annonces officielles chinoises, tous les passagers des vols en provenance de la Chine ont dès Janvier 2020 été soumis à un contrôle de température. Tous les cas suspects sont alors assignés à résidence en isolement avec contrôle du

signal de leur téléphone afin de garantir que l'appareil ne quitte pas le domicile. Plusieurs appels sont par ailleurs passés chaque jour par les services de sécurité de manière aléatoire pour s'assurer que les habitants infectés sont bien chez eux.

Chine

A l'origine de la propagation du virus, la Chine a très rapidement utilisé son impressionnant arsenal technologique pour pister les cas de contamination à travers le pays. Au delà d'un confinement localisé autour des poches d'infections, chaque citoyen s'est vu assigner un QR code changeant de couleur (rouge/vert) en fonction du risque contagieux de l'individu. Calculé par algorithme de manière opaque et prenant en compte des paramètres tels que les contacts, les déplacements effectués ou l'historique des paramètres de santé, le QR code permet à chacun d'avoir accès ou non aux transports, magasins, résidences ou services publics.

Ce code couleur est par ailleurs relié au système national de reconnaissance faciale s'appuyant sur plus de 300 millions de caméras de surveillance à travers le pays. Couplées à des capteurs thermiques dans les foyers d'infections, ces caméras permettent aux autorités de détecter et traquer par géolocalisation des smartphones tout cas suspect ou de surveiller les comportements des citoyens comme sur le port du masque par exemple. Centralisées au niveau national, ces informations permettent d'alimenter le système de notation sociale en cours de déploiement au sein de la population. Assignant à chaque citoyen 100 points, les autorités distribuent ainsi bonus ou malus à chacun en fonction de son comportement avec toutes les conséquences imaginables sur la vie quotidienne. C'est un peu la version moderne de la carotte et du bâton au pays du petit livre rouge faisant passer la série Black Mirror pour un compte pour enfant.

Le pouvoir s’appuie en parallèle sur les tristement fameux comités de quartier créés en 1950 par le pouvoir communiste pour contrôler la population. Le pays est ainsi subdivisé en millions de cellules. Chaque bâtiment, rue, quartier, entreprise, village ou ville a son comité de surveillance reconnaissable par un brassard rouge ayant tout pouvoir de contrôle et délation sur leur cellule. Ce maillage étroit du pays s’assure notamment du bon respect de la quarantaine pour chacun ou du droit d’accès, n’hésitant pas à poser des mouchards électroniques sur les portes des étrangers ou des habitants venant d’ailleurs.

Corée du Sud

En guerre contre la corée du Nord, les autorités ont par ailleurs juridiquement un droit total d’accès aux données privées des citoyens en cas de risque sanitaire depuis l’épidémie de SRAS. Très tôt prise au sérieux, la lutte contre la pandémie s’est appuyée sur une politique massive de tests avec isolement immédiat de tous les cas suspects. Chaque personne infectée est géolocalisée par l’intermédiaire de son téléphone pour s’assurer du bon respect de son isolement. Son activité digitale et son historique de déplacement sont analysés. Les données telles que les lieux fréquentés, les heures de passage, le genre ou l'âge sont rendues publiques et réutilisées par la société civile pour alerter les individus ou créer de nombreux services privés de lutte contre la pandémie. Un système de notification avertit notamment en cas de risque de contagion les Sud Coréens ayant été en contact.

Hong Kong

Dès l’atterrissage un bracelet électronique est remis à chaque passager par les autorités. Couplé à une application qu’il a obligation de télécharger, chaque individu est ainsi traqué pour s’assurer du bon respect de la quarantaine. Au delà des voyageurs, ce système s’étend désormais à tous les cas d’infection.

Pologne

Comme dans de nombreux pays à travers la planète, la Pologne impose à toute personne suspecte du fait d'une infection ou d'un risque de contagion, une quarantaine stricte de 14 jours à domicile. Elle peut alors choisir de manière libre entre le téléchargement d'une application, Home Quarantine, lui demandant de se prendre en selfie de manière aléatoire plusieurs fois par jour ou le passage des forces de l'ordre pour vérifier du bon respect de sa quarantaine. Le pays a dans ses projets une seconde application non obligatoire, ProteGO, ayant vocation à informer les citoyens d'un risque de contagion. Souhaitant utiliser la technologie Bluetooth, le gouvernement a dû mettre le projet en stand-by dans l'attente de la plateforme Apple-Google permettant d'accéder à la technologie.

Israël

Habitué à la lutte anti-terroriste, le gouvernement a confié au Shin-Beth (services de sécurité intérieure) la lutte contre la propagation du virus. Analyse massive des données privées, géolocalisation des téléphones, utilisation de drones et des systèmes de surveillance du pays pour traquer la population, tous les moyens sont utilisés. La population est mise sous surveillance pour mieux la protéger selon le discours officiel. Chacun peut ainsi recevoir un SMS lui donnant ordre de se mettre en quarantaine sans plus d'explication et malheur à ceux ne respectant pas les consignes. Les milieux ultra-orthodoxes en ont déjà fait les frais.

Singapour

Citée en exemple par les promoteurs de StopCovid, l'application mise en place par les autorités de Singapour n'a cependant pas permis aux autorités d'éviter la mise en quarantaine de la Cité-Etat. Téléchargée à ce jour par moins de 20% de la population, TraceTogether est basée sur la

technologie bluetooth pour détecter la proximité avec une personne infectée. Chacun peut télécharger librement l'application. Le numéro de téléphone local est alors relié à un identifiant. L'application garde en mémoire l'historique des personnes rencontrées et enregistre la liste des contacts de chacun. En cas d'identification d'un cas suspect, les équipes de contact tracking passent en revue l'historique de chacun pour alerter les contacts d'une potentielle infection.

Chronique d'un échec annoncé

Ayant passé en revue les outils mis en place par les différents pays dans la lutte contre la pandémie, force est de constater que le respect de l'anonymat et des données privées n'est pas vraiment la priorité. A part pour les régimes autoritaires, le succès est loin d'être au rendez-vous. Quelles sont les pistes envisagées pour l'application StopCovid ?

Basée sur une technologie Bluetooth, l'application lancée par les pouvoirs publics, n'aurait aucun caractère obligatoire et permettrait d'alerter chacun d'un risque potentiel de contagion en cas de contact avec une personne infectée. Simplement dans cette définition, l'initiative porte déjà avant sa naissance les germes de son échec. Utilisant des trésors de diplomatie dans les choix stratégiques de peur des réactions, les promoteurs politiques ou privés accumulent les choix les plus critiquables.

Bluetooth

La technologie Bluetooth est très imprécise et ne permet pas de connaître précisément la distance entre chaque utilisateur. A cela s'ajoute une contrainte technique liée aux utilisateurs d'iPphone et du système d'exploitation IoS d'Apple qui n'autorise pas une application à utiliser de manière autonome et continue le bluetooth. Cela obligera les utilisateurs

à télécharger une mise à jour du système d'exploitation du téléphone pour pouvoir utiliser l'application. Les choix techniques posent questions au vu des objectifs affichés. Ils répondent objectivement plus à des critères politiques que d'efficacité.

Prenant de vitesse les États, Apple et Google ont annoncé un partenariat technologique sur le sujet permettant de toucher près de 99% des smartphones en circulation sur la planète. Basé sur une plateforme inter-opérable entre Android et IOS, le système permettrait de lever les barrières imposées aux développeurs de la planète autour de l'utilisation du Bluetooth. Sur le papier extrêmement séduisante, cette initiative pose pourtant de nombreux problèmes.

Respectant l'anonymat de chacun et ne transférant aucune information à des serveurs centraux, cette initiative mécontente fortement le gouvernement en lui supprimant tout accès aux données et d'une certaine manière remettant en cause sa souveraineté. Ne voulant pas céder face à Apple, les promoteurs de StopCovid sont aujourd'hui au point mort des négociations. Plusieurs gouvernements ont d'ailleurs en Europe décidé d'attendre le lancement officiel de la plateforme début Mai avant de se positionner.

Technologiquement très intéressante par la liberté donnée à chacun sur l'utilisation de ses données et une garantie d'anonymat qu'aucun gouvernement ne peut promettre de manière crédible, cette initiative va susciter à raison un vrai débat. En effet, les deux géants américains se retrouvent, de fait, en véritable position de force dans des négociations avec les gouvernements de la planète, et notamment face à l'Europe. Même si la solution proposée peut être d'une grande efficacité technologique, comment ne pas imaginer celle-ci comme un cheval de Troie ? Elle ouvre une autoroute à la digitalisation de nos données de santé qui se retrouveraient ainsi dans des mains américaines. Vous conviendrait que ceci est très difficile à assumer politiquement en période

de reconquête de la souveraineté nationale.

Non obligatoire

Les enjeux sont tels que la recherche d'une efficacité optimale est plus que prioritaire. Pour ce faire, toutes les études sur le sujet montrent qu'un taux d'utilisation minimum de 65% à 70% est nécessaire. Aïe… C'est ici que les chiffres font mal et les mathématiques rendent l'équation particulièrement complexe. Le caractère non contraignant de l'application par prudence politique et obligation légale (loi européenne sur la protection des données privées célèbre sous le doux nom de RGPD oblige) mettent à la merci du diktat de l'opinion publique les chances de succès.

Le taux d'équipement de la population en smartphone était en 2019 de 77% selon une étude du Crédoc. Cela veut dire que 23% de la population n'a pas de smartphone à ce jour. Nous en sommes donc à 100% - 23% (ceux ne pouvant pas télécharger l'application pour des raisons techniques) = 77% de la population pouvant potentiellement télécharger l'application.

Un Sondage Odoxa du 13 avril 2020 en partenariat avec l'Usine Digitale révèle que 62% de la population française serait prête à télécharger une application de type StopCovid. Si l'on reprend nos calculs, 62% de 77 (% de la population pouvant télécharger l'application) = 47,74 % de la population.

Simplement sur ces deux critères, moins de la moitié de la population téléchargerait l'application à ce jour. Vous me direz que je suis de mauvaise foi, de nombreuses personnes ayant répondu au sondage pouvant ne pas avoir pris en compte le fait qu'elles n'ont pas de smartphone. L'argument est pertinent. Mais pourtant ne change pas la réalité des chiffres.

En effet, ces chiffres ne prennent pas en compte les zones blanches françaises, où peu voire aucun réseau ne passe. En 2018 et selon l'association UFC Que Choisir, celles-ci représentaient 6,8 millions d'habitants soit un peu plus de 10% de la population française. A cela doivent être comptabilisés les chiffres des personnes pouvant avoir des difficultés à télécharger l'application au sein des personnes âgées notamment.

En synthèse, même dans les meilleurs scénarios, il est utopique d'espérer un taux de téléchargement supérieur à 50% de la population française ce qui compromet fortement la pertinence du dispositif. Jamais je n'aurais cru être d'accord un jour avec Jean Luc Mélenchon !

Pouvoirs publics

Là est peut-être la partie du projet me rendant le plus perplexe : un contrôle par les pouvoirs publics. Par où commencer tant les arguments sont nombreux pour décrédibiliser le donneur d'ordre ?

Qui se souvient de l'application SAIP lancée en grande pompe sous la présidence Hollande suite aux attentats de 2015 en France et en prévision de l'Euro de football ? Le dispositif sous forme d'application permettait de relayer des informations prioritaires en cas de péril majeur auprès de la population. D'un coût de plus de 300 000 euros le ministère de l'intérieur a décidé après deux ans de mettre fin au projet devant la succession de dysfonctionnements particulièrement gênants pour l'Etat, allant d'un taux extrêmement faible de téléchargements à un délai de réactivité supérieur à 2 heures lors des attaques perpétrées à Nice sur la promenade des Anglais le 14 Juillet 2018. Cela fait désordre. Permettez-moi a priori de ne pas donner quitus à la puissance publique sur le sujet !

Le gouvernement avance l'effacement des données de plus de 15 jours et un code informatique rendu public pour rassurer. Encore une fois les

promesses n’engagent que ceux qui y croient. L’histoire récente ne joue pas en sa faveur sur le sujet. Les lois d’exception votées suite aux attentats de 2015 se sont retrouvées à caractère permanent avec un dispositif de contrôle de la totalité des communications de la population. Des boîtes noires algorithmiques sont depuis reliées à tous les opérateurs télécoms fournissant au ministère de l’intérieur des renseignements sur les individus ayant un comportement considéré comme suspect. Malgré les nombreuses demandes formulées par la société civile sur les critères pris en compte pour définir la dangerosité des individus, aucune réponse n’a été donnée quels que soient les gouvernements. Circulez il n’y a rien à voir !

Mettre à disposition de l’État une application dont les règles du jeu pourront changer demain sans crier gare alors que la presse aura les yeux tournés sur la prochaine crise me semble particulièrement dangereux dans le climat de haute tension dans lequel le pays se trouve. Le comportement des forces de l’ordre épuisées après des mois de conflits est très révélateur et ne contribue pas à rassurer. Dans un climat où le ministre de l’intérieur français se félicite d’avoir verbalisé plus de 800 000 personnes pour non respect du confinement, les abus de pouvoir de plus en plus nombreux des représentants de l’autorité publique participent à l’hystérisation du débat. Comment ne pas s'interroger sur la possibilité d’utiliser StopCovid demain à des fins de surveillance plus autoritaire ? L’Etat ne peut être juge et parti.

Autre sujet de préoccupation particulièrement grave, l’utilisation des données. La révélation il y a quelques jours de l’intention du gouvernement d’autoriser la transmission de nos données de santé à l’américain Palantir dans le cadre de la lutte contre la pandémie ne facilite pas un climat de confiance. Fournisseur du Pentagone, de la CIA, de la NSA, et des services secrets de nombreux pays de la planète, notamment français, la startup est connue pour une utilisation massive des algorithmes et des données privées pour aider ses clients à créer de

la valeur et à identifier la bonne information. Synonyme de tracking agressif, l'annonce est plus que malheureuse en plein débat sur l'indépendance stratégique de la Nation.

Confier un potentiel tracking social à un opérateur privé tel Orange, les GAFA ou le conglomérat européen travaillant à une solution n'est pas plus crédible. L'opérateur de télécommunication leader en France vient en effet de sortir du bois par la voix de son PDG en annonçant avoir finalisé une application pouvant être mise à la disposition du gouvernement. Quelles sont les garanties d'indépendance, de non utilisation commerciale ou même de réussite ?

Une application ne serait pourtant pas une si mauvaise idée à certaines conditions. Mon père m'a toujours appris que toute critique ne pouvait être valable que si elle est accompagnée de propositions constructives. Les voici. Revenons aux fondamentaux.

Quelles seraient les conditions du succès d'une application respectant nos libertés fondamentales ?

La relecture de "l'art de la guerre" de Sun Tzu nous apprend qu'avant toute tactique il faut définir une stratégie. Cela tombe bien, nous sommes en guerre !

Quelles sont les objectifs de l'application ?

Couplée à une politique massive de tests de la population, une application de lutte contre la pandémie doit permettre à chacun d'être informé d'un risque de contagion afin d'être soi-même testé, mis en isolement afin de ne pas contaminer et suivi par une équipe médicale compétente. Les

objectifs fondamentaux sont donc simples : INFORMATION et PRÉVENTION en temps réel. Un opérateur indépendant et reconnu à la manoeuvre : la CNIL

Indépendantes de l'état et des intérêts privés, la CNIL et son équivalent européen l'EDPB sont déjà garants de la bonne utilisation des données privées. Ils ont en la matière une solide réputation et les compétences nécessaires pour être les donneurs d'ordre d'une solution emportant l'engouement de la population.

Responsabiliser la population

Peut-être est-il temps comme en Allemagne ou Suède de responsabiliser la population au lieu de la stigmatiser pour son attitude potentiellement irresponsable. Pensez-vous sérieusement qu'une personne recevant l'information qu'elle a été exposée à une potentielle contamination irait risquer sa vie et celle des autres en n'allant pas elle-même se faire dépister et ainsi se soumettre à un protocole médical adapté ? Inutile de ficher les gens et créer une usine à gaz d'enquêtes ou de chasse à l'Homme !

Blockchain et cryptage

L'anonymat doit être la règle ! Aucun fichier ne doit être centralisé, aucune donnée privée exportée, aucune liste de contacts téléchargée. Pour ce faire la technologie Blockchain peut être une piste intéressante. Elle permettrait, en étant couplée à un cryptage de bout en bout telle qu'utilisé par l'application Telegram, de garantir l'anonymat et le respect des fondamentaux. Aucun organisme ni prestataire ne pourrait avoir accès à une liste des personnes infectées, leurs contacts, leurs habitudes ou leur genre. Seule information à être délivrée au bon destinataire et lui seul : le risque d'infection. Le reste serait traité en local sur le smartphone de chacun.

Géolocalisation

A partir du moment où l’anonymat est garanti, et qu’il n’y a aucun risque de tracking d’un historique de localisation par des opérateurs humains, la technologie de géolocalisation doit être utilisée. Seul un positionnement précis de chacun permettra au système d’évaluer un risque de contact avec une personne infectée et donc une efficacité de prévention.

QR code

Chaque test effectué pourrait donner accès à un QR code scannable sur l’application par le laboratoire d’analyse médical, l'hôpital ou le médecin. En cas d’infection, l’application pourrait sur le smartphone comparer avec les informations fournies par la blockchain pour identifier et alerter les personnes à risque en renvoyant l’information sur la blockchain.

Notification de la population et médecine de proximité

Connecté en permanence à la blockchain, chaque utilisateur serait informé en temps réel par une notification en cas de risque d’infection l’invitant au plus vite à aller se faire dépister. Le médecin référent pourrait alors être le contact privilégié afin de prendre en charge rapidement le patient. Un back-up de sécurité pourrait intervenir dans l’hypothèse où le patient ne réagit pas dans les 24h suivant la première notification (scan du QR code de l’application) en renvoyant une seconde notification et une alerte potentielle au médecin référent soumis au secret médical.

Simplicité d’usage et automatisation sans intervention humaine

La simplicité d’usage, la rapidité et l’automatisation complète du système sont des critères prioritaires de succès. Inutile de réinventer la poudre. Il suffit de s’inspirer des meilleures pratiques internationales dans le domaine des applications et de s’appuyer sur l’existant pour concevoir

rapidement un système robuste et efficace. L’absence du traitement de l’information par l’humain, de sa centralisation et donc des risques associés de détournement de cette information à des objectifs détournés permettrait une adhésion massive du public. L’enjeu majeur de l’application est sa réactivité et la transmission de l’information. Elle permettrait en ciblant uniquement la chaîne de contagion, de réduire drastiquement le taux de contagion du virus donc à affaiblir la propagation de la pandémie.

Arrêtons de faire passer des vessies pour des lanternes. Il est totalement faux de faire croire à la population que sa sécurité sanitaire implique l’abandon de ses droits fondamentaux à la liberté et à l’anonymat. Non je ne téléchargerai pas l’application StopCovid ! Non je n’ai pas l’intention de me laisser intimider par une moralisation rampante d’une opinion publique terrorisée et prête à accepter toute proposition court termiste, quel qu’en soit le prix ! Des solutions pragmatiques existent. Elles doivent s’appuyer sur l’existant et être détachées du pouvoir politique. Résistons à l’hystérie collective et gardons notre sang-froid. Il est plus que temps de montrer ce que l’Homme est capable de faire collectivement en s’adaptant comme il l’a fait de tout temps aux contraintes extérieures.

Jean-Christophe Bonis est co-fondaeur d'Isabo et conférencier

---

Article écrit par Jean-Christophe Bonis