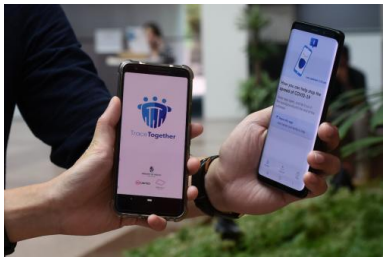
Surveillance de l'épidémie: attention au «solutionnisme technologique»

PAR GÉRALDINE DELACROIX
ARTICLE PUBLIÉ LE VENDREDI 3 AVRIL 2020



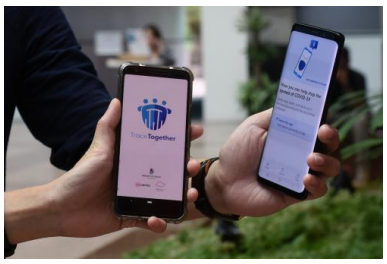
Démonstration de l'application TraceTogether à Singapour, le 20 mars. © Catherine LAI / AFP

Alors que le gouvernement envisage la création d'une application de suivi des contacts des uns et des autres pour prévenir les contaminations, Annie Blandin et Charles-Pierre Astolfi, du Conseil national du numérique, relèvent le besoin de « *garanties démocratiques particulièrement fortes* » et plaident pour « *une logique d'entraide, de confiance* ».

Comment protéger la population de la contamination par le coronavirus autrement qu'en enfermant chacun chez soi ? Comment protéger, aussi, ceux qui sont obligés de poursuivre leurs déplacements, malgré le confinement ? Pour un groupe de chercheurs d'Oxford dont **l'étude** a été publiée dans la revue *Science* le 31 mars, « *la dissémination virale est trop rapide pour être contenue* » par des enquêtes « *manuelles* » de suivi des personnes contacts. Mais confier cette mission à une application pourrait y remédier, disent les chercheurs, à condition qu'elle soit utilisée par un nombre suffisamment grand de personnes.

C'est la piste que semble vouloir suivre le gouvernement français. « *On étudie ce qui se fait ailleurs, notamment à Singapour, mais aussi au Royaume-Uni et en Allemagne. Pour le moment, rien n'est en place. Pas une ligne de code n'est écrite* », **expliquait aux *Échos*** le secrétariat d'État au numérique le 31 mars. « *On pourrait peut-être, sur le fondement d'un engagement volontaire, utiliser ces méthodes pour mieux tracer la circulation du virus et les contacts de chacun, mais nous n'avons pas aujourd'hui d'instrument légal qui rendrait obligatoire ce tracking* », a précisé (regretté ?) le premier ministre, Édouard Philippe, lors de son audition devant l'Assemblée, mardi 1er avril.

Cette stratégie avait été évoquée pour la première fois le 24 mars, lors de l'annonce, par la présidence de la République, de la mise en place du Comité analyse recherche et expertise (Care), chargé, entre autres, « *de conseiller le gouvernement pour ce qui concerne les programmes et la doctrine relatifs aux traitements, aux tests et aux pratiques de "backtracking" qui permettent d'identifier les personnes en contact avec celles infectées par le virus du Covid-19* ». Une identification passant par des outils numériques : le comité « *accompagnera par ailleurs la réflexion des autorités* […] *sur l'opportunité de la mise en place d'une stratégie numérique d'identification des personnes ayant été au contact de personnes infectées* », poursuivait le communiqué.



Démonstration de l'application TraceTogether à Singapour, le 20 mars. © Catherine LAI / AFP

L'application **TraceTogether**, développée par le gouvernement de Singapour, sert de modèle à tous. Fondée sur la technologie Bluetooth, qui détecte les appareils environnants (par exemple pour connecter un téléphone à une enceinte musicale), elle enregistre sur les téléphones des utilisateurs les appareils se trouvant à proximité. Lorsqu'une personne dotée de l'application se déclare contaminée, celles qu'elle a côtoyées sont prévenues – sans être informées de l'identité de la personne en question.

Ainsi, un consortium « *pan-européen* » dans lequel figure l'Inria, l'Institut national pour la recherche numérique, s'est constitué « *pour aider les initiatives nationales* » à travailler à la mise en œuvre d'une application du même type, se voulant respectueuse de la vie privée, sous le nom barbare de **PEPP PT** (Pan-European Privacy-Preserving Proximity Tracing).

Pendant ce temps, Orange et l'Inserm ont fait connaître les modalités de leur **partenariat** sur les données de géolocalisation, tandis que Google a décidé de présenter des **indicateurs de mobilité** construits grâce aux données *« agrégées et anonymisées »* de ses utilisateurs, et ce dans plus de 130 pays dont la France.

Enfin, dernière initiative « numérique » en date, le ministère de l'intérieur a annoncé un dispositif d'attestation de sortie disponible sur smartphone, qui soulève lui aussi quelques questions. Selon le communiqué du ministère, un fichier pdf sera créé dans le smartphone de l'utilisateur (*« aucune information saisie dans le formulaire n'est enregistrée sur un quelconque serveur »*) et lu à distance grâce à un QR Code par le fonctionnaire chargé du contrôle. Que deviendront ces infos dans le terminal policier ? Interrogé vendredi par Mediapart, le ministère répond que *« pour scanner les attestations, les forces de l'ordre utilisent les tablettes et smartphones NEO en possession de la quasi totalité des patrouilles maintenant. L'attestation de déplacement dérogatoire s'affiche sur le lecteur des forces de l'ordre »*. Ce qui ne répond pas clairement à la question de savoir ce qui se passe après cet affichage.

Face à cette ébullition en matière de contrôle informatisé, nous nous sommes tournés vers le Conseil national du numérique (CNNum), pour savoir ce que l'on pensait de tout cela au sein de cet organisme placé sous l'autorité du secrétaire d'État du numérique et chargé *« d'informer et de conseiller le gouvernement »*, mais aussi *« de formuler de manière indépendante* […] *des avis et des recommandations »*.

Charles-Pierre Astolfi, son secrétaire général, et Annie Blandin, spécialiste du droit européen du numérique, ont répondu ensemble à nos questions.

Vous avez entamé un recensement des différentes applications de traçage et de surveillance à travers le monde. Qu'avez-vous constaté jusqu'à présent ?

Charles-Pierre Astolfi. © DR

Charles-Pierre Astolfi : Il y a traçage et traçage. Dans les applications qui existent déjà, et dans celles qui sont encore à l'étude, on peut définir deux extrêmes. Il y a à la fois l'initiative pan-européenne PEPP PT, qui respecte apparemment très bien la confidentialité des données et qui pousse l'anonymat au maximum. Et à côté de ça, il y a l'application qu'utilise la Pologne : si vous êtes en quarantaine, soit vous avez des visites impromptues de la police, qui vérifie que vous êtes bien chez vous, soit l'application vous envoie une notification impromptue aussi, et vous devez faire un selfie pour prouver que vous êtes bien chez vous.

Le gouvernement français a-t-il sollicité le CNNum pour la mise en place de sa stratégie ?

C.-P. A. : Non, il n'y a pas eu de saisine officielle du CNNum sur le sujet.

Néanmoins, vous y réfléchissez ?

C.-P. A. : Oui, il existe au CNNum une réflexion sur ces questions. On a publié ce matin un premier **guide de bonnes pratiques** pour ceux qui développent des initiatives, pas spécialement sur les applications de traçage mais en général, sur les applications d'entraide, de solidarité.

Quels sont les points importants à sécuriser en matière de respect de la vie privée ?

Annie Blandin : Tout dépend des données que vont traiter les différentes applications. S'agit-il de données de santé, de données de géolocalisation, de données

Bluetooth ? Si on reprend le projet pan-européen, c'est davantage un projet fondé sur le traitement de données Bluetooth. C'est un premier point.

Annie Blandin. © DR

Ce qu'il faut sécuriser, c'est effectivement la gestion des données personnelles, ça, c'est évident. Mais nous, on estime aussi qu'il faut des garanties démocratiques particulièrement fortes, compte tenu du contexte, qui doivent amener à clarifier l'objectif de l'usage du numérique dans le contexte de la politique sanitaire. C'est-à-dire qu'il faut bien insister sur le rôle complémentaire, sur les limites, aussi, du système. Il faut fonder un tel système sur un ensemble de valeurs. À la différence de systèmes qui sont fondés sur la surveillance explicite, ici, on serait plus dans une logique d'entraide, de confiance, d'inclusion numérique, avec l'idée d'associer vraiment le citoyen à sa propre protection, à la protection des autres, ainsi qu'à la santé publique.

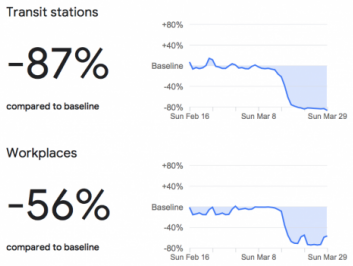
L'idée qu'on pourrait suivre, c'est de s'appuyer sur les initiatives citoyennes et sur la bonne volonté des citoyens pour aborder tout ça de manière collective. Voilà une piste de réflexion.

Quels résultats peut-on attendre, par exemple, d'une application du type de celle utilisée à Singapour ?

C.-P. A. : À Singapour, à peu près 10 % de la population a installé l'application. Est-ce que c'est suffisant ? Ce sont les épidémiologistes qui peuvent le dire. Ce qui est sûr, c'est que plus il y en a, mieux c'est. C'est 10 % dans un pays où le taux de pénétration du smartphone est supérieur à celui de la France. Voilà pour le contexte.

Il ne faut pas verser dans le solutionnisme technologique. On ne fait pas une application parce que les autres pays le font… On fait une application si on pense que ça peut aider dans une politique de santé publique. C'est là qu'il faut se demander de quoi on a besoin, quel est le parc qui doit être installé, quelle est la proportion des gens qui doivent l'utiliser pour que ce soit utile, etc. Ce ne sont pas des décisions techniques.

Le conseil scientifique et le Care doivent se prononcer sur les scénarios de fin de confinement. J'espère qu'ils produiront ce genre d'analyse.



Ces graphiques bâtis par Google montrent la chute des déplacements en France, dans les transports en commun et vers les lieux de travail. © Google

Une telle appli, qui est présentée comme un outil pour gérer la sortie du confinement, pourrait-elle être utile avant ? Faut-il attendre ?

C.-P. A. : Ce que j'ai vu à l'étranger, c'est que souvent ces applications, comme TraceTogether à Singapour, sont associées à des politiques de dépistage systématique. Donc il faut être capable de faire les deux.

A. B. : En termes de risques, justement, il y a aussi ce risque de se sentir à tort en sécurité, dans la mesure où ce sont de toute façon des systèmes non universels, que les gens utiliseraient volontairement, et sous réserve qu'ils soient équipés de smartphones.

Le secret médical semble être le grand oublié de ce débat…

A. B. : Les personnes peuvent consentir au traitement de leurs données de santé. Dans ce cas, il n'y a aucun problème.

C.-P. A. : Deux remarques. D'abord, le secret médical s'applique aux médecins et pas aux patients. Si le patient est d'accord, il peut dire à sa famille, à qui il veut, même sur Facebook, qu'il a la grippe. La

deuxième chose, c'est qu'il faut inscrire ce genre d'application dans des démarches de santé publique beaucoup plus générales.

Par exemple, en Corée du Sud, de très nombreux fonctionnaires ont été mobilisés pour faire uniquement de l'enquête, demander à chaque personne infectée qui elle avait rencontré les 14 jours précédents et pour recontacter toutes ces personnes. Tracer les cas potentiels, ce n'est pas qu'une question d'application, cela peut se faire avec ou sans. L'application, c'est la continuité de l'enquête.

A. B. : Dès qu'on parle de ces applications, dès qu'on parle de l'usage potentiel du numérique pour la gestion de cette crise, on pense données personnelles, mais les données de santé sont aussi des données d'intérêt général. Et tout l'enjeu, c'est de les traiter comme des données d'intérêt général, sans pour autant, évidemment, mettre en péril la protection des données personnelles et de la vie privée.

Des traitements de données ont déjà été mis en place, comme le travail que l'Inserm conduit avec des données de géolocalisation fournies par Orange. Aujourd'hui, Google met en ligne des graphiques issus des données de géolocalisation de ses utilisateurs. Ces opérations présentent-elles des risques en matière de fuites de données ?

C.-P. A. : Avec Orange et Google, on est dans le cadre de données qui sont à la fois anonymisées et agrégées. Il y a donc très très peu de risques. On obtient des moyennes et, à la fin, on a un graphe, quelque chose de très très macro. On ne peut pas remonter à la donnée personnelle. Ce ne sont pas les données agrégées d'Orange qui vont dire que je suis resté à Paris et que mon collègue est parti dans sa maison de campagne…

A. B. : Il s'agit là de données agrégées et anonymisées. Alors, bien sûr, l'anonymisation, ça n'est pas un processus parfait, loin s'en faut. On le sait, alors peut-être ne faut-il pas hésiter à le dire ! Parce qu'il y a aussi un besoin très fort de transparence dans cette période, sur les opportunités que peuvent représenter certaines actions, et sur les risques. Il y a vraiment un besoin d'être très très clair sur les risques.

Boite noire

L'entretien a été réalisé vendredi 3 avril avec WhatsApp, puis relu et amendé à la marge. C'est ma collègue Camille Polloni qui a contacté le ministère de l'intérieur. La réponse du ministère a été ajoutée dans la soirée, quand elle nous est parvenue.

Directeur de la publication : Edwy Plenel
Direction éditoriale : Carine Fouteau et Stéphane Alliès
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 24 864,88€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Laurent Mauduit, Edwy Plenel (Président), Sébastien Sassolas, Marie-Hélène Smiéjan, François Vitrani. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart, Société des salariés de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 24 864,88€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.