

StopCovid

Dieu ou diable ?

Pierre angulaire du processus de déconfinement, le traçage numérique soulève des interrogations politiques, réglementaires, technologiques et éthiques. Malgré les risques encourus, les options ne sont finalement pas si nombreuses pour prévenir une seconde vague épidémique. Faute de mieux, il faudra juger sur pièce.

Les libertés individuelles et collectives seront-elles sacrifiées sur l'autel de la santé publique ? Dans un pays d'inspiration jacobine, le débat est passionné. Pierre angulaire du processus de déconfinement, le traçage numérique doit créer du lien entre les trois grands axes de la stratégie gouvernementale, à savoir « protéger, dépister et isoler ». L'enjeu consiste à prévenir les conséquences d'une seconde vague épidémique, qui serait dramatique sur le plan sanitaire, économique et psychologique.

Deux dispositifs numériques sont en cours de déploiement : un système d'information de proximité et une application mobile. Lancé le 13 mai, Contact Covid doit notamment faciliter l'identification des cas potentiels dans l'environnement proche d'un patient contaminé par le nouveau coronavirus (voir encadré). Plus controversée, StopCovid doit élargir le champ de la recherche à l'ensemble de ses interactions dans la société civile, via son smartphone. Confié à l'Inria fin avril, le développement de l'outil s'avère complexe, essentiellement pour des raisons technologiques. Un temps remise en question, sa généralisation pourrait finalement intervenir dans la foulée du débat parlementaire, qui devait débiter le 27 mai.

Un choix technologique contesté

Contrairement à la Chine ou à la Corée du Sud, où traçage rime avec « flitage », la France a choisi la méthode douce. Les informations les plus sensibles seront stockées sur un serveur central, dont la gestion sera confiée à une autorité sanitaire publique qui n'a pas encore été désignée. Le gouvernement a décidé de se passer des services de Google et d'Apple, quitte à freiner la conception



Un temps remise en question, la généralisation de StopCovid pourrait finalement intervenir le 2 juin, à l'issue d'un débat parlementaire très attendu.

ou la diffusion de sa propre application. Le choix d'un système centralisé ne fait pas l'unanimité. « Il aurait été plus simple et plus rapide de collaborer et de s'appuyer sur l'expertise technologique de ces deux opérateurs spécialisés. Sous réserve d'un encadrement strict de la coopération, il n'y avait pas de risque majoré pour la gestion et le traitement des données », explique Patrice Navarro, counsel au sein du cabinet Hogan Lovells LLP.

Moins « liberticide » que la géolocalisation ou le bornage téléphonique, le Bluetooth a également été privilégié, en dépit des inconvénients techniques et pratiques. « StopCovid devra fonctionner en continu pour récolter et transférer des informations. Les batteries devraient se vider rapidement, ce qui pourrait décourager de nombreux utilisateurs, comme ce fut le cas avec l'application singapourienne », affirme-t-il. Autre limite redoutée : une moindre précision du traçage, avec des résultats variables et aléatoires. « L'utilisateur qui recevra l'alerte ne saura pas où le contact s'est produit. Il ne pourra donc pas le restituer dans son contexte pour évaluer le risque. A titre d'exemple, il lui sera impossible de se souvenir ou de déterminer si la personne contaminée portait

ou non un masque de protection », indique Ariane Mole, avocate associée au sein du cabinet Bird&Bird.

Une base légale solide, mais...

Critiquée, la démarche est pourtant parfaitement légale. En cas de menace avérée sur la santé publique, le gouvernement peut user de la loi ou du règlement pour réquisitionner des données sensibles ou restreindre les libertés individuelles et collectives. « Malgré la remise en cause de certains droits fondamentaux, un dispositif de traçage numérique peut être généralisé, sans être contraire au RGPD », rappelle Ariane Mole, qui a récemment participé à la rédaction d'un livre blanc sur le sujet¹. Le consentement de la personne n'est pas systématiquement un gage de conformité, même pour une application aussi intrusive que StopCovid.

Les pouvoirs publics devront néanmoins s'assurer du respect des règles juridiques, à commencer par les modalités de traitement et de conservation des données, qui ne pourront pas excéder la durée de l'épidémie. Ils devront également préciser la finalité, le fonctionnement et les usages de l'outil. La réponse proposée devra par ailleurs être proportionnée et utile, ce qui n'a rien d'évident en l'état.

« Il y a aujourd'hui une contradiction manifeste entre le principe d'utilité et le volontariat, qui réduit de fait l'intérêt de cette application. Une faible adhésion la rendrait inutile, donc non nécessaire », souligne Patrice Navarro. Le gouvernement pourra toujours fixer ses propres conditions dans le cadre législatif, état d'urgence sanitaire oblige. Il pourra imposer cette solution numérique, comme le port obligatoire du masque dans les transports en commun, y compris de manière coercitive.

Le défi de l'adhésion

Dans un avis publié le 26 avril, la CNIL² formulait ses premières recommandations. Consentement éclairé, temporalité limitée, suppression possible des données, désinstallation rapide et immédiate de l'application... Sans surprise, elle privilégiait également un accès facultatif. Ce dernier point interroge cependant sur l'efficacité même de ce dispositif de traçage, dont le potentiel sera inévitablement bridé. « On ne peut pas laisser reposer des enjeux de santé publique sur le volontariat », juge Ariane Mole, citant le cas des zones grises et des personnes non équipées d'un smartphone, qui constituent déjà

« un obstacle majeur à sa diffusion ». Plus d'un tiers de la population serait hors-jeu d'office.

La logique est arithmétique : pour être utile, l'application devra être très largement utilisée. De ce point de vue, la partie est loin d'être gagnée. Les dernières enquêtes d'opinion témoignent d'un enthousiasme modéré. Selon l'étude réalisée par l'observatoire Data Publica³, moins de la moitié des sondés envisagent de télécharger StopCovid (49 %). Très peu d'entre eux sont même sûrs de le faire (15 %). Parmi les principaux freins évoqués, les personnes interrogées craignent pour l'exploitation de leurs données (54 %), une réticence notamment liée à un manque d'information sur ce sujet (67 %). Seul véritable modèle comparable, l'exemple singapourien ne prête pas à l'optimisme. Le taux d'adhésion est inférieur à 20 %.

Des verrous multiples

Les nombreuses zones d'ombre autour de ce projet alimentent un sentiment de défiance légitime. « Faute de transparence, l'outil développé a un caractère anxiogène. Les patients ne s'en servent pas, sauf sous la

contrainte, ce qui serait d'autant plus dommageable », déplore Gérard Raymond, président de France Assos Santé. « La non-concertation aura noyé le sentiment de responsabilité. Le sacrifice de nos libertés fondamentales aurait mérité quelques explications », ironise-t-il.

Au regard des enjeux, le facteur humain semble avoir été négligé. La santé numérique ne peut pas se fonder sur une approche mécanique, déshumanisée, voire culpabilisante. « Cette initiative inédite requiert un accompagnement circonstancié. La sensibilisation et l'information du grand public devront être améliorées, en particulier sur les technologies mobilisées et leur niveau de sécurité. Les Français ont besoin d'être rassurés », constate Paul Frappé, président du Collège de médecine générale. Assez paradoxalement, StopCovid pourrait avoir des répercussions contre-productives. « Le nombre de tests disponibles sera-t-il suffisant pour couvrir un échantillon populationnel aussi large ? », s'interroge-t-il. L'application pourrait non seulement fragiliser les capacités de dépistage du pays, mais également alourdir le circuit de

>>>



Jean-Carles Grelier, député LR de la Sarthe : « Une approche antidémocratique et contre-productive »

Quelle doit être la place du traçage numérique dans la stratégie de déconfinement ?

● Cette méthode relève de l'empirisme. Elle ne repose sur aucun fonde-

ment scientifique solide. C'est une démarche palliative destinée à sauver les apparences. La réalité est bien plus prosaïque : le gouvernement n'a pas été capable de mobiliser les ressources suffisantes pour dépister et protéger la population. La douloureuse gestion des masques en témoigne. Les professionnels de santé ont dû faire des appels aux dons, voire financer eux-mêmes leurs équipements de protection. Malgré la hausse récente des capacités nationales, il ne s'agit toujours pas d'une priorité stratégique. Le traçage numérique ne changera rien. C'est une mauvaise réponse à une vraie question.

Certains outils sont-ils plus pertinents que d'autres ?

● Peu importe la solution déployée, ce sera un gâchis de temps et d'argent public. Plus grave, certaines valeurs fondamentales seront bafouées, à commencer par le respect du secret médical. La restriction des libertés individuelles et collectives est particulièrement préoccupante. La crise sanitaire ne justifie pas tout. Les Français sont atta-

chés à leurs données de santé. Ils doivent pouvoir en disposer comme bon leur semble. Ils ne céderont pas aux sirènes de la peur et de la contrainte. Les dispositifs proposés sont intrusifs et anxiogènes. Ils ne présentent aucune garantie en matière de sécurité. Certains d'entre eux sont d'une complexité et d'une inefficacité telles qu'ils pourraient bien ne jamais voir le jour, à l'instar de StopCovid, dont l'utilité est contestée au sein même de la majorité.

L'exploitation des données de santé peut-elle réellement contribuer à réduire le risque épidémique ?

● La prise de risque est démesurée par rapport à la finalité. La réglementation ne nous protégera pas des cybercriminels ni des GAFAM. A défaut d'être exploitées commercialement, nos données de santé pourraient servir à entraîner des algorithmes ou alimenter la recherche privée sur l'intelligence artificielle. Elles pourraient tout aussi bien être vendues aux plus offrants sur des marchés parallèles. Il est trop dangereux de les rendre accessibles à des tiers, même indirectement et partiellement, au nom de l'intérêt public en santé. Une notion plutôt abstraite qui n'a d'ailleurs pas été véritablement définie.

Propos recueillis par Jonathan Icart

>>>

prise en charge. A l'instar des "faux positifs", les "faux contacts" pourrait même accentuer cette pression...

Une prise de risque

De toute évidence, le traçage numérique est une opération à haut risque. « Les pouvoirs publics devront faire preuve d'une vigilance renforcée pour préserver les intérêts de la population et de la santé publique. La sécurité informatique doit être une priorité absolue », prévient Paul Frappé. La pseudonymisation et les nouveaux algorithmes de cryptographie n'y changeront rien : le respect total de l'anonymat ne pourra pas être totalement garanti. « Aussi protectrice soit-elle, la réglementation et la technologie ne nous

préservent pas d'éventuelles attaques extérieures, commanditées par des cybercriminels expérimentés », relève Gérard Raymond. Même indirecte, la présence des GAFAM suscite toujours la méfiance. « Leurs méthodes sont douteuses. En tant que support de téléchargement, ils pourraient facilement récupérer des fragments de données pour alimenter leurs projets. La santé doit être sanctuarisée. Elle doit impérativement être placée au-dessus des lois du marché. »

En l'absence d'un traitement ou d'un vaccin, les solutions pour contenir la propagation du virus ne sont pas légion. La situation est exceptionnelle. La prise de risque l'est tout autant. Elle pourrait même avoir valeur de jurisprudence, en

légitimant une pratique pour le moins discutable, mais encore peu discutée. La boîte de Pandore va bientôt s'ouvrir. Qu'en sortira-t-il ? ■

Jonathan Icart

(1) « Bird&Bird & Data Protection – Livre blanc sur les options possibles en protection des données personnelles pour le déploiement d'applications mobiles dans la lutte contre la pandémie de Covid-19 », Bird&Bird (avril 2020).

(2) Commission nationale de l'informatique et des libertés – CNIL.

(3) « Perceptions de l'application StopCovid et regards sur l'enjeu du partage des données personnelles », Data Publica/Harris Interactive (mai 2020).



© Inria / Pierre Morel

Bruno Sportisse, pdg de l'Inria* :

« Mettre le numérique au service de la lutte contre la pandémie »

Quelles seront les principales fonctionnalités de StopCovid ?

- Chaque smartphone muni de StopCovid va générer des crypto-identifiants

éphémères, d'une durée de quinze minutes. Une fois activée, l'application pourra détecter et conserver** ceux des utilisateurs rencontrés, sous la forme d'un historique de proximité, propre à chaque appareil.

Quelles seront les données transmises au serveur central ?

- Géré par une autorité sanitaire, le serveur central ne contiendra que les historiques de proximité à risque, autrement dit ceux des utilisateurs dont les smartphones ont croisé les smartphones des utilisateurs diagnostiqués positifs. Une condition toutefois : la personne contaminée aura dû volontairement renseigner une preuve de son diagnostic dans l'application de manière sécurisée, par exemple via un QR code.

De quelle manière les recoupements seront-ils effectués ?

- A intervalles réguliers, l'application vérifiera si ses propres crypto-identifiants se trouvent parmi les historiques de proximité à risque, disponibles sur le serveur. Le cas échéant, elle affichera une notification sur le smartphone de l'utilisateur concerné, en lui proposant la conduite à tenir, comme appeler un numéro vert ou aller consulter un médecin.

Quelles sont les différences fondamentales avec les solutions développées par Google et Apple ?

- Ces deux opérateurs n'ont pas conçu une appli, mais une boîte à outils pour les développeurs. Dans ce schéma, chaque utilisateur peut recevoir dans son application les crypto-identifiants de tous les utilisateurs diagnostiqués positifs. Outre la nature de ce modèle, les solutions développées sur cette base ne permettent pas à l'autorité sanitaire de contrôler deux variables essentielles dans la gestion de la pandémie : la régulation et l'efficacité du déploiement de l'application.

La collaboration a-t-elle été totalement interrompue ?

- C'est impossible pour une simple et bonne raison : Android et iOS sont les systèmes d'exploitation les plus répandus en France. Ils équipent la totalité des terminaux mobiles, à peu de choses près. Nous discutons régulièrement avec ces deux sociétés pour faciliter le développement et la diffusion de StopCovid.

Comment comptez-vous garantir l'intégrité des données ?

- Nous avons respecté les cadres légaux français et européen, à commencer par le RGPD. L'application repose sur une installation volontaire et une pseudonymisation des données, de sorte que personne ne puisse être capable de retracer la liste des personnes testées positives ni de reconstituer la chaîne de contamination. Nous avons également des échanges récurrents avec la CNIL.

Quid de la cybersécurité ?

- Pour nous prémunir d'éventuelles attaques malveillantes, nous avons notamment utilisé le dernier cri des algorithmes de cryptographie. Comme dans tout système informatique, des failles peuvent exister. Associée au projet depuis le premier jour, l'implication de l'ANSSI aura été et sera déterminante pour les rendre inopérantes.

Propos recueillis par Jonathan Icart

(*) L'Institut national de recherche en sciences et technologies du numérique coordonne l'équipe projet StopCovid, officiellement lancée le 26 avril dernier. Elle est composée d'instituts recherche (Inserm), d'acteurs publics (Santé publique France, ANSSI) et de sociétés privées (Capgemini, Dassault Systèmes, Lunabee Studio, Orange et Withings, 3DS).

(**) L'application ne stocke que son propre historique de proximité et aucune autre donnée.