

Covid-19. Enjeux techniques de l'application de traçage numérique StopCovid

Description

Lancée le 2 juin 2020 sur les magasins d'applications d'Apple et de Google, StopCovid, l'application française de suivi de contact s'appuie notamment sur le Bluetooth et le protocole ROBERT, visant à garantir à ses utilisateurs l'anonymat que requiert ce projet et à établir une indépendance numérique vis-à-vis de Google et d'Apple.

Finalité du projet

Le suivi de contact, en anglais *contact tracing*, fait partie du protocole utilisé par les équipes médicales afin de retracer, *via* leurs déplacements, les rencontres des personnes contaminées lors d'une pandémie, dans le but d'identifier d'autres personnes éventuellement infectées et de reconstituer les chaînes de contamination. Ce suivi de contact était effectué jusqu'alors sur le terrain par le personnel médical en face à face avec les malades. Un taux d'équipement en smartphones de la population française supérieur à 75 % a permis d'envisager de numériser les chaînes de contamination grâce à une application mobile, comme ont choisi de le faire l'Allemagne, le Royaume-Uni, l'Italie, la Suisse ou encore l'Estonie.

Nommée StopCovid, l'application mobile française de suivi de contact permet de reconstituer automatiquement les liens de transmission de la maladie afin de prévenir ceux et celles qui ont croisé une personne contaminée et de les inciter, notamment, à réaliser un test de dépistage. Cet outil numérique devrait servir à prévenir une éventuelle seconde vague de contamination survenant après le déconfinement du 11 mai 2020.

Proposée sur les magasins d'applications de Google et d'Apple à compter du 2 juin 2020, l'installation de l'application s'appuie sur le volontariat. Lorsque deux personnes ayant préalablement installé l'application sur leur smartphone se croisent pendant au minimum 15 minutes, à une distance de moins d'un mètre, leurs appareils se détectent *via* leur connexion Bluetooth et enregistrent leurs identifiants respectifs qui seront conservés durant 14 jours. Par la suite, si une personne s'avère malade, elle pourra le déclarer *via* l'application, selon une procédure stricte permettant d'éviter de fausses déclarations, et alertant ainsi automatiquement toutes les personnes dont l'identifiant aura été enregistré dans son smartphone.

Les choix techniques de la France

Depuis le 7 avril 2020, l'Inria (Institut national de recherche en sciences et technologies du numérique), sous la supervision du ministère des solidarités et de la santé et du secrétariat d'État chargé du numérique, en lien avec le ministère de l'enseignement supérieur, de la recherche et de l'innovation, est chargé de

piloter le développement de l'application, auquel contribuent, à titre gracieux, des acteurs publics et privés, notamment l'Anssi (Agence nationale de la sécurité des systèmes d'information, Inserm (Institut national de la santé et de la recherche médicale), Santé Publique France, Capgemini, Dassault Systèmes, Lunabee, Orange et Withings.

Bluetooth vs géolocalisation

Une application de suivi de contact basée sur la géolocalisation de l'appareil apparaissant comme contraire aux impératifs d'anonymisation, le choix s'est porté sur le Bluetooth Low Energy, qui permet à deux smartphones de se détecter à une distance rapprochée et d'échanger leurs identifiants respectifs. En utilisant l'outil d'analyse d'Exodus Privacy, association à but non lucratif dont l'objet est d'avoir « *une meilleure compréhension des enjeux liés au pistage par le biais des applications Android* » ([voir La rem n°45, p.57](#)), il s'avère que l'installation de StopCovid sur un smartphone requiert onze permissions, dont notamment, en plus du Bluetooth, l'accès à la géolocalisation, pourtant écartée par les instigateurs du projet. Il faut y voir une impossibilité technique, la France ayant fait le choix d'éviter de passer par la solution clé en main, proposée par Apple et Google. Dès la fin mars 2020, chacun de son côté, puis conjointement à partir du 10 avril 2020, Apple et Google ont travaillé à la création d'une API (*Application Programming Interface*) afin de permettre aux développeurs et aux États de créer une application de suivi de contact exonérée des limitations techniques qu'ils imposent habituellement. Ainsi, la solution américaine garantit l'activation de la seule liaison Bluetooth, proscrivant même l'accès de l'application aux autres services de géolocalisation.

En revanche, une application tierce comme StopCovid reste soumise aux contraintes des systèmes d'exploitation américains, l'accès au Bluetooth ne pouvant être dissocié d'une permission d'accès à tous les autres services de localisation, même si, dans la pratique, seul le Bluetooth sera utilisé. Apple interdit d'autre part aux applications qui sont ouvertes, mais fonctionnent en arrière-plan, d'accéder au Bluetooth, pour notamment protéger la vie privée des utilisateurs et la durée de vie de la batterie. L'application de suivi de contact, utilisée à Singapour, TraceTogether, conçue sur le modèle de StopCovid, illustre parfaitement cet écueil : les personnes équipées d'un iPhone sont contraintes de relancer constamment l'application, comme l'explique le site d'information Frandroid.

Approche centralisée vs décentralisée

L'API fournie par Apple et Google, nommée Exposure Notification, fonctionne sur un modèle « décentralisé », c'est-à-dire que les identifiants de chaque utilisateur sont générés par l'application, stockés directement sur les smartphones et circulent entre chaque appareil lorsqu'un utilisateur s'est déclaré malade. Comme l'indique Émile Marzolf, rédacteur pour acteurpublics.fr : « *Dans un modèle décentralisé, l'identification des contacts qu'a pu avoir une personne testée positive est réalisée directement de smartphone à smartphone, là où, dans le modèle centralisé, les informations remontent toutes vers un serveur central, de manière pseudonymisée, pour être comparées.* » Exposure Notification de Google et Apple est utilisée par les instances de santé publique de vingt-deux pays à ce jour afin de développer leur

application de suivi de contact et d'en définir précisément les modalités d'usage. La Suisse teste l'application SwissCovid depuis le 18 mars 2020 et son lancement officiel est prévu fin juin 2020. Depuis le 8 juin 2020, l'Italie expérimente l'application Immuni dans quatre régions test. L'Allemagne propose l'application Corona-Warn-App depuis le 16 juin 2020.

Afin de protéger sa souveraineté numérique, la France, a préféré une approche centralisée, s'appuyant sur un protocole développé par l'Inria et l'institut allemand Fraunhofer pour la sécurité appliquée et intégrée (AISEC). Baptisé ROBERT (ROBust and privacy-presERving proximity Tracing), ce protocole émane d'une collaboration franco-allemande dans le cadre de l'initiative européenne PEPP-PT (Pan European Privacy-Preserving Proximity Tracing), qui a pour objet la création d'outils de suivi de contact respectueux des réglementations européennes en matière de protection des données, de vie privée et de sécurité ([voir La rem n°48, p.20](#)).

Selon Bruno Sportisse, président de l'Inria, *« 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 »*. Il n'en reste pas moins que l'application s'appuie sur un serveur central où sont stockés tous les identifiants pseudonymes des personnes exposées à la maladie. La Direction générale de la santé (DGS) en est le garant, tandis que les données sont hébergées en France par 3DS/Outscale. Selon Stéphane Le Calme, chroniqueur pour le site [developpez.com](#), ce serveur central sert à générer l'identifiant unique de chaque utilisateur : *« Cet identifiant doit rester le plus secret possible si le gouvernement veut assurer ses promesses d'anonymat. Pour que l'identifiant soit difficilement attribuable à un smartphone (et donc à une personne), StopCovid va embarquer un module de chiffrement de cet identifiant. Un algorithme va chiffrer à intervalle régulier l'identifiant unique. À chaque fois, l'identifiant unique sera donc chiffré d'une manière différente. »*

Hubert Guillaud, rédacteur en chef d'InternetActu.net de la Fondation Internet Nouvelle Génération (FING) estime, pour sa part, que *« rien ne nous dit que la police et les autorités de santé n'auront jamais accès aux données. Rien ne nous dit non plus que les données collectées par de telles applications de « contact tracking » ne pourraient pas être « désanonymisées »*. En effet, il suffirait à un gouvernement de croiser les données de tous les utilisateurs pour reconstituer les allées et venues d'une grande partie des citoyens *« volontaires »*. Quant à la Cnil, dont la délibération a été rendue publique le 24 avril 2020 (voir *supra*), elle préconisait, à l'instar de l'Anssi, le remplacement de l'algorithme de chiffrement de l'identifiant des utilisateurs par un autre, réputé plus sûr. Néanmoins, le Sénat et l'Assemblée nationale ont approuvé sans modification l'application StopCovid le 27 mai 2020.

Cependant, le 13 juin 2020, Gaëtan Leurent, chercheur français en cryptographie, qui participe au développement de l'application StopCovid au sein de l'Inria, a découvert que lorsqu'un utilisateur se déclare malade, *« tous les contacts croisés pendant les 14 derniers jours »* sont envoyés au serveur central, et non *« uniquement les contacts avec un risque de transmission, c'est-à-dire à moins d'un mètre pendant plus de 15 minutes »*. Le fonctionnement de l'application StopCovid semble ainsi être en contradiction avec le principe de minimisation posé par la Cnil et le Règlement général sur la protection des données personnelles (RGPD) qui prévoient que *« les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »*

. Le secrétariat d'État chargé du numérique, au courant de la situation, justifie cependant ce fonctionnement dans des propos rapportés par Mediapart : *« tous les quarts d'heure, un nouvel identifiant est attribué à chaque appareil. [...] Ainsi, un contact qui ne durerait que cinq minutes pourrait être la suite d'un contact de douze minutes : deux contacts que seul le serveur est capable de relier pour comprendre qu'il s'agit en réalité d'un seul, de 17 minutes, donc à risques. »* Des explications qui ne convainquent pas le lanceur d'alerte, pour qui des moyens techniques relativement simples permettraient de résoudre ce problème. Gaëtan Leurent y voit une *« contradiction avec le décret qui encadre l'utilisation de StopCovid »* et également *« un vrai risque »* que le serveur apprenne le graphe social des utilisateurs.

Les enjeux techniques sont des choix politiques

En optant pour une solution maison, la France montre sa volonté de s'émanciper de l'offre américaine, indépendamment des garanties avancées par celle-ci. À l'inverse, l'Allemagne s'est désolidarisée de l'utilisation du protocole ROBERT, lui préférant l'API de Google et Apple, à l'instar de 22 pays parmi lesquels l'Italie, la Suisse ou les Pays-Bas. La solution choisie par la France, qui implique une centralisation des données, présente pourtant, selon l'avis d'experts en sécurité, un risque plus élevé de piratage. Les choix techniques du développement de l'application StopCovid ont fait naître d'importantes tensions au sein même de l'État, entre les partisans de la solution proposée par les géants du web et le protocole promu par l'Inria, allant jusqu'à écarter du projet la Direction interministérielle du numérique (Dinum).

À vouloir concilier objectif de traçage numérique, respect des libertés publiques et souveraineté nationale, finalement aucune solution technique, notamment en pair-à-pair, garantissant vraiment l'anonymat des utilisateurs, n'aura été proposée au gouvernement français. De plus, les applications de suivi de contact sont indissociables des moyens humains et sanitaires mis en œuvre pour lutter efficacement contre la Covid-19. Présidente de la Cnil depuis février 2019, Marie-Laure Denis, auditionnée par le Sénat le 15 avril 2020, appelait à *« la vigilance sur le solutionnisme technologique »* ([voir La rem n°33, p.60](#)) en rappelant qu'il était *« dangereux de penser qu'une application de ce type peut tout résoudre »*.

L'application StopCovid n'est qu'une mesure de lutte contre la Covid-19 parmi d'autres, et son utilité dépendra forcément de son taux d'utilisation dans le temps. Le premier bilan tiré de la mise en œuvre d'une application de suivi de contact à Singapour, en Australie ou en Islande est loin d'être encourageant. Ainsi Jason Bay, directeur de l'agence gouvernementale des services numériques de Singapour, où l'application TraceTogether est disponible depuis le 20 mars 2020, assène : *« Si vous me demandez si n'importe quelle application de traçage, existante ou en développement, n'importe où dans le monde, va remplacer le traçage manuel, je dirais sans hésitation que la réponse est non. »*

Sources :

- « Covid-19 : la vie privée sera-t-elle une victime collatérale de l'épidémie de coronavirus ? », Fabien Soyez, cnetfrance.fr, 10 avril 2020.
- « Covid-19 : Bluetooth, serveur central, logiciel libre... On en sait un peu plus sur StopCovid », Alice Vitard, usine-digitale.fr, 20 avril 2020.

-
- « Entre Bubble et Apollo, la petite histoire du traçage commun d'Apple et de Google », Mickaël Bazoge, igen.fr, 28 avril 2020.
 - « Application StopCovid : la France isolée dans son bras de fer avec Apple et Google », Damien Leloup, *Le Monde*, 28 avril 2020.
 - « Recours aux Gafam, centralisation : les choix techniques sur StopCovid ont attisé les tensions au sein de l'État », Émile Marzolf, acteurspublics.fr, 30 avril 2020.
 - « StopCovid ou encore ? » Cedric 0, medium.com, 3 mai 2020.
 - « Centralisé ou décentralisé : quelles différences entre les architectures des apps de contact tracing ? », François Manens, numerama.com, 5 mai 2020.
 - « StopCovid, toutes les réponses à vos questions sur l'application du déconfinement », frandroid.com, 7 mai 2020.
 - « Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n° 20008032) », cnil.fr, 25 mai 2020. « StopCovid : l'INRIA va remplacer l'algorithme de chiffrement de l'application de contact tracing », Stéphane le Calme, developpez.com, 25 mai 2020.
 - « Dans quel cas l'app StopCovid sera-t-elle efficace ? », Marie Turcan, numerama.com, 27 mai 2020.
 - « Application StopCovid : que sait-on du projet français de traçage des contacts ? », Julien Lausson, numerama.com, 28 mai 2020.
 - « Application StopCovid : accouchée dans la douleur, et une efficacité déjà remise en cause », Sylvain Tronchet, franceinter.fr, 30 mai 2020.
 - « FAQ sur les aspects techniques de l'application StopCovid », inria.fr, 1^{er} juin 2020.
 - « StopCovid demande l'accès à la géolocalisation sur Android, mais s'engage à ne pas l'utiliser », Julien Lausson, numerama.com, 2 juin 2020.
 - « Too much contact data sent to the server », Gaëtan Leurent, [GitLab](https://gitlab.com), Inria.fr, June 12, 2020.
 - « StopCovid, l'appli qui en savait trop », Géraldine Delacroix, mediapart.fr, 15 juin 2020.
 - « L'application StopCovid collecte plus de données qu'annoncé », *Le Monde*, 16 juin 2020.

Categorie

1. Techniques

date créée

18 juillet 2020

Auteur

jacquesandrefines