Covid-19.Â Enjeux techniques de lâ€™application de traÃ§age numÃ©rique StopCovid

Description

LancÃ©e le 2 juin 2020 sur les magasins dâ€™applications dâ€™Apple et de Google, StopCovid, lâ€™application franÃ§aise de suivi de contact sâ€™appuie notamment sur le Bluetooth et le protocole ROBERT, visant Ã garantir Ã ses utilisateurs lâ€™anonymat que requiert ce projet et Ã Ã©tablir une indÃ©pendance numÃ©rique vis-Ã -vis de Google et dâ€™Apple.

FinalitÃ© du projet

Le suivi de contact, en anglaisÂ *contact tracing*, fait partie du protocole utilisÃ© par les Ã©quipes mÃ©dicales afin de retracer,*Â viaÂ* leurs dÃ©placements, les rencontres des personnes contaminÃ©es lors dâ€™une pandÃ©mie, dans le but dâ€™identifier dâ€™autres personnes Ã©ventuellement infectÃ©es et de reconstituer les chaÃ®nes de contamination. Ce suivi de contact Ã©tait effectuÃ© jusquâ€™alors sur le terrain par le personnel mÃ©dical en face Ã face avec les malades. Un taux dâ€™Ã©quipement en smartphones de la population franÃ§aise supÃ©rieur Ã 75 % a permis dâ€™envisager de numÃ©riser les chaÃ®nes de contamination grÃ¢ce Ã une application mobile, comme ont choisi de le faire lâ€™Allemagne, le Royaume-Uni, lâ€™Italie, la Suisse ou encore lâ€™Estonie.

NommÃ©e StopCovid, lâ€™application mobile franÃ§aise de suivi de contact permet deÂ reconstituer automatiquement les liens de transmission de la maladie afin de prÃ©venir ceux et celles qui ont croisÃ© une personne contaminÃ©eÂ et de les inciter, notamment, Ã rÃ©aliser un test de dÃ©pistage. Cet outil numÃ©rique devrait servir Ã prÃ©venir une Ã©ventuelle seconde vague de contamination survenant aprÃ¨s le dÃ©confinement du 11 mai 2020.

ProposÃ©e sur les magasins dâ€™applications de Google et dâ€™Apple Ã compter du 2 juin 2020, lâ€™installation de lâ€™application sâ€™appuie sur le volontariat. Lorsque deux personnes ayant prÃ©alablement installÃ© lâ€™application sur leur smartphone se croisent pendant au minimum 15 minutes, Ã une distance de moins dâ€™un mÃ¨tre, leurs appareils se dÃ©tectentÂ *viaÂ* leur connexion Bluetooth et enregistrent leurs identifiants respectifs qui seront conservÃ©s durant 14 jours. Par la suite, si une personne sâ€™avÃ¨re malade, elle pourra le dÃ©clarerÂ *viaÂ* lâ€™application, selon une procÃ©dure stricte permettant dâ€™Ã©viter de fausses dÃ©clarations, et alertant ainsi automatiquement toutes les personnes dont lâ€™identifiant aura Ã©tÃ© enregistrÃ© dans son smartphone.

Les choix techniques de la France

Depuis le 7 avril 2020, lâ€™Inria (Institut national de recherche en sciences et technologies du numÃ©rique), sous la supervision du ministÃ¨re des solidaritÃ©s et de la santÃ© et du secrÃ©tariat dâ€™Ã‰tat chargÃ© du numÃ©rique, en lien avec le ministÃ¨re de lâ€™enseignement supÃ©rieur, de la recherche et de lâ€™innovation, est chargÃ© de piloter le dÃ©veloppement de lâ€™application, auquel contribuent, Ã titre gracieux, des acteurs publics et privÃ©s, notamment l'Anssi (Agence nationale de la sÃ©curitÃ© des systÃ¨mes d'information, Inserm (Institut national de la santÃ© et de la recherche mÃ©dicale), SantÃ© Publique France, Capgemini, Dassault SystÃ¨mes, Lunabee, Orange et Withings.

BluetoothÂ *vs*Â gÃ©olocalisation

Une application de suivi de contact basÃ©e sur la gÃ©olocalisation de lâ€™appareil apparaissant comme contraire aux impÃ©ratifs dâ€™anonymisation,Â le choix sâ€™est portÃ© sur le Bluetooth Low Energy, qui permet Ã deux smartphones de se dÃ©tecter Ã une distance rapprochÃ©e et dâ€™Ã©changer leurs identifiants respectifs.Â En utilisant lâ€™outil dâ€™analyse dâ€™Exodus Privacy, association Ã but non lucratif dont lâ€™objet est dâ€™avoirÂ *Â«Â une meilleureÂ comprÃ©hension des enjeux liÃ©s au pistage par le biais des applications AndroidÂ Â»*Â (voirÂ *La rem*Â nÂ°45, p.57), il sâ€™avÃ¨re queÂ lâ€™installation de StopCovid sur un smartphone requiert onze permissions,Â dont notamment, en plus du Bluetooth, lâ€™accÃ¨s Ã la gÃ©olocalisation, pourtant Ã©cartÃ©e par les instigateurs du projet. Il faut y voir une impossibilitÃ© technique, la France ayant fait le choix dâ€™Ã©viter de passer par la solution clÃ© en main, proposÃ©e par Apple et Google. DÃ¨s la fin mars 2020, chacun de son cÃ´tÃ©, puis conjointement Ã partir du 10 avril 2020, Apple et Google ont travaillÃ© Ã la crÃ©ation dâ€™une APIÂ *(Application Programming Interface)*Â afin de permettre aux dÃ©veloppeurs et aux Ã‰tats de crÃ©er une application de suivi de contact exonÃ©rÃ©e des limitations techniques quâ€™ils imposent habituellement. Ainsi, la solution amÃ©ricaine garantit lâ€™activation de la seule liaison Bluetooth, proscrivant mÃªme lâ€™accÃ¨s de lâ€™application aux autres services de gÃ©olocalisation.

En revanche, une application tierce comme StopCovid reste soumise aux contraintes des systÃ¨mes dâ€™exploitation amÃ©ricains,Â lâ€™accÃ¨s au Bluetooth ne pouvant Ãªtre dissociÃ© dâ€™une permission dâ€™accÃ¨s Ã tous les autres services de localisation, mÃªme si, dans la pratique, seul le Bluetooth sera utilisÃ©. Apple interdit d'autre part aux applications qui sont ouvertes, mais fonctionnent en arriÃ¨re-plan, dâ€™accÃ©der au Bluetooth, pour notamment protÃ©ger la vie privÃ©e des utilisateurs et la durÃ©e de vie de la batterie. Lâ€™application de suivi de contact, utilisÃ©e Ã Singapour, TraceTogether, conÃ§ue sur le modÃ¨le de StopCovid, illustre parfaitement cet Ã©cueil : les personnes Ã©quipÃ©es dâ€™un iPhone sont contraintes de relancer constamment lâ€™application, comme lâ€™explique le site dâ€™information Frandroid.

Approche centralisÃ©eÂ *vs*Â dÃ©centralisÃ©e

Lâ€™API fournie par Apple et Google, nommÃ©e Exposure Notification, fonctionne sur un modÃ¨leÂ Â«Â dÃ©centralisÃ©Â Â», câ€™est-Ã -dire que les identifiants de chaque utilisateur sont

gÃ©nÃ©rÃ©s par lâ€™application, stockÃ©s directement sur les smartphones et circulent entre chaque appareil lorsquâ€™un utilisateur sâ€™est dÃ©clarÃ© malade. Comme lâ€™indique Ã‰mile Marzolf, rÃ©dacteur pour acteurpublics.fr :Â *Â«Â Dans un modÃ¨le dÃ©centralisÃ©, lâ€™identification des contacts quâ€™a pu avoir une personne testÃ©e positive est rÃ©alisÃ©e directement de smartphone Ã smartphone, lÃ oÃ¹, dans le modÃ¨le centralisÃ©, les informations remontent toutes vers un serveur central, de maniÃ¨re pseudonymisÃ©e, pour Ãªtre comparÃ©es.Â Â»*Â Exposure Notification de Google et Apple est utilisÃ©e par les instances de santÃ© publique de vingt-deux pays Ã ce jour afin de dÃ©velopper leur application de suivi de contact et dâ€™en dÃ©finir prÃ©cisÃ©ment les modalitÃ©s dâ€™usage. La Suisse teste lâ€™application SwissCovid depuis le 18 mars 2020 et son lancement officiel est prÃ©vu fin juin 2020. Depuis le 8 juin 2020, lâ€™Italie expÃ©rimente lâ€™application Immuni dans quatre rÃ©gions test. Lâ€™Allemagne propose lâ€™application Corona-Warn-App depuis le 16Â juin 2020.

Afin de protÃ©ger sa souverainetÃ© numÃ©rique, la France, a prÃ©fÃ©rÃ© une approche centralisÃ©e,Â sâ€™appuyant sur un protocole dÃ©veloppÃ© par lâ€™Inria et lâ€™institut allemand Fraunhofer pour la sÃ©curitÃ© appliquÃ©e et intÃ©grÃ©e (AISEC). BaptisÃ© ROBERT (ROBust and privacy-presÂERving proximity Tracing), ce protocole Ã©mane dâ€™une collaboration franco-allemande dans le cadre de l'initiative europÃ©enne PEPP-PT (Pan European Privacy-Preserving Proximity Tracing), qui a pour objet la crÃ©ation dâ€™outils de suivi de contact respectueux des rÃ©glementations europÃ©ennes en matiÃ¨re de protection des donnÃ©es, de vie privÃ©e et de sÃ©curitÃ© (voirÂ *La rem* Â nÂ°48, p.20).

Selon Bruno Sportisse, prÃ©sident de lâ€™Inria,Â *Â«Â sa conception permet que personne, pas mÃªme lâ€™Ã‰tat, nâ€™ait accÃ¨s Ã la liste des personnes diagnostiquÃ©es positives ou Ã la liste des interactions socialesÂ Â»*. Il nâ€™en reste pas moins queÂ lâ€™application sâ€™appuie sur un serveur central oÃ¹ sont stockÃ©s tous les identifiants pseudonymes des personnes exposÃ©es Ã la maladie.Â La Direction gÃ©nÃ©rale de la santÃ© (DGS) en est le garant, tandis que les donnÃ©es sont hÃ©bergÃ©es en France par 3DS/Outscale. Selon StÃ©phane Le Calme, chroniqueur pour le site developpez.com, ce serveur central sert Ã gÃ©nÃ©rer lâ€™identifiant unique de chaque utilisateur :Â *Â«Â Cet identifiant doit rester le plus secret possible si le gouvernement veut assurer ses promesses dâ€™anonymat. Pour que lâ€™identifiant soit difficilement attribuable Ã un smartphone (et donc Ã une personne), StopCovid va embarquer un module de chiffrement de cet identifiant. Un algorithme va chiffrer Ã intervalle rÃ©gulier lâ€™identifiant unique. Ã€ chaque fois, lâ€™identifiant unique sera donc chiffrÃ© dâ€™une maniÃ¨re diffÃ©rente.Â Â»*

Hubert Guillaud, rÃ©dacteur en chef d'InternetActu.net de la Fondation Internet Nouvelle GÃ©nÃ©ration (FING) estime, pour sa part, queÂ *Â«Â rien ne nous dit que la police et les autoritÃ©s de santÃ© nâ€™auront jamais accÃ¨s aux donnÃ©es. Rien ne nous dit non plus que les donnÃ©es collectÃ©es par de telles applications deÂ Â«Â* contact trackingÂ *Â»Â ne pourraient pas Ãªtre Â«Â dÃ©sanonymisÃ©esÂ Â». En effet, il suffirait Ã un gouvernement de croiser les donnÃ©es de tous les utilisateurs pour reconstituer les allÃ©es et venues dâ€™une grande partie des citoyensÂ Â«Â volontaires*

Â«Â *Â Â*». Quant Ã la Cnil, dont la dÃ©libÃ©ration a Ã©tÃ© rendue publique le 24 avril 2020 (voir *Â supra*), elle prÃ©conisait, Ã lâ€™instar de lâ€™Anssi, le remplacement de lâ€™algorithme de chiffrement de lâ€™identifiant des utilisateurs par un autre, rÃ©putÃ© plus sÃ»r. NÃ©anmoins, le SÃ©nat et lâ€™AssemblÃ©e nationale ont approuvÃ© sans modification lâ€™application StopCovid le 27 mai 2020.

Cependant, le 13 juin 2020, GaÃ«tan Leurent, chercheur franÃ§ais en cryptographie, qui participe au dÃ©veloppement de lâ€™application StopCovid au sein de lâ€™Inria, a dÃ©couvert que lorsquâ€™un utilisateur se dÃ©clare malade,Â *Â«Â tous les contacts croisÃ©s pendant les 14 derniers joursÂ Â»*Â sont envoyÃ©s au serveur central, et nonÂ *Â«Â uniquement les contacts avec un risque de transmission, câ€™est-Ã -dire Ã moins dâ€™un mÃ¨tre pendant plus de 15 minutesÂ Â»*. Le fonctionÂnement de lâ€™application StopCovid semble ainsi Ãªtre en contradiction avec le principe de minimisation posÃ© par la Cnil et le RÃ¨glement gÃ©nÃ©ral sur la protection des donnÃ©es personnelles (RGPD) qui prÃ©voient queÂ *Â«Â les donnÃ©es Ã caractÃ¨re personnel doivent Ãªtre adÃ©quates, pertinentes et limitÃ©es Ã ce qui est nÃ©cessaire au regard des finalitÃ©s pour lesquelles elles sont traitÃ©esÂ Â»*. Le secrÃ©tariat dâ€™Ã‰tat chargÃ© du numÃ©rique, au courant de la situation, justifie cependant ce fonctionnement dans des propos rapportÃ©s par Mediapart :Â *Â«Â tous les quarts dâ€™heure, un nouvel identifiant est attribuÃ© Ã chaque appareil.Â* [â€¦]*Â Ainsi, un contact qui ne durerait que cinq minutes pourrait Ãªtre la suite dâ€™un contact de douze minutes : deux contacts que seul le serveur est capable de relier pour comprendre quâ€™il sâ€™agitÂ en rÃ©alitÃ© dâ€™un seul, de 17 minutes, donc Ã risques.Â Â»*Â Des explications qui ne convainquent pas le lanceur dâ€™alerte, pour qui des moyens techniques relativement simples permettraient de rÃ©soudre ce problÃ¨me. GaÃ«tan Leurent y voit uneÂ *Â«Â contradiction avec le dÃ©cret qui encadre l'utilisation de StopCovidÂ Â»*Â et Ã©galementÂ *Â«Â un vrai risqueÂ Â»*Â 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 volontÃ© de sâ€™Ã©manciper de lâ€™offre amÃ©ricaine, indÃ©pendamment des garanties avancÃ©es par celle-ci. Ã€ lâ€™inverse, lâ€™Allemagne sâ€™est dÃ©solidarisÃ©e de lâ€™utilisation du protocole ROBERT, lui prÃ©fÃ©rant lâ€™API de Google et Apple, Ã lâ€™instar de 22 pays parmi lesquels lâ€™Italie, la Suisse ou les Pays-Bas. La solution choisie par la France, qui implique une centralisation des donnÃ©es, prÃ©sente pourtant, selon lâ€™avis dâ€™experts en sÃ©curitÃ©, un risque plus Ã©levÃ© de piratage.Â Les choix techniques du dÃ©veloppement de lâ€™application StopCovid ont fait naÃ®tre dâ€™importantes tensions au sein mÃªme de lâ€™Ã‰tat,Â entre les partisans de la solution proposÃ©e par les gÃ©ants du web et le protocole promu par lâ€™Inria, allant jusquâ€™Ã Ã©carter du projet la Direction interministÃ©rielle du numÃ©rique (Dinum).

Ã€ vouloir concilier objectif de traÃ§age numÃ©rique, respect des libertÃ©s publiques et souverainetÃ© nationale, finalement aucune solution technique, notamment en pair-Ã -pair, garantissant vraiment lâ€™anonymat des utilisateurs, nâ€™aura Ã©tÃ© proposÃ©e au gouvernement franÃ§ais. De plus, les

applications de suivi de contact sont indissociables des moyens humains et sanitaires mis en Å“uvre pour lutter efficacement contre la Covid-19. PrÃ©sidente de la Cnil depuis fÃ©vrier 2019, Marie-Laure Denis, auditionnÃ©e par le SÃ©nat le 15 avril 2020, appelait Ã Â *Â«Â la vigilance sur le solutionnisme technologiqueÂ Â»*Â (voirÂ *La rem*Â nÂ°33, p.60) en rappelant quâ€™il Ã©taitÂ *Â«Â dangereux de penser qu'une application de ce type peut tout rÃ©soudreÂ Â»*.

Lâ€™application StopCovid nâ€™est quâ€™une mesure de lutte contre la Covid-19 parmi dâ€™autres, et son utilitÃ© dÃ©pendra forcÃ©ment de son taux dâ€™utilisation dans le temps.Â Le premier bilan tirÃ© de la mise en Å“uvre dâ€™une application de suivi de contact Ã Singapour, en Australie ou en Islande est loin dâ€™Ãªtre encourageant.Â Ainsi JasonÂ Bay, directeur de lâ€™agence gouvernementale des services numÃ©riques de Singapour, oÃ¹ lâ€™application TraceTogether est disponible depuis le 20 mars 2020, assÃ¨ne :Â *Â«Â Si vous me demandez si nâ€™importe quelle application de traÃ§age, existante ou en dÃ©veloppement, nâ€™importe oÃ¹ dans le monde, va remplacer le traÃ§age manuel, je dirais sans hÃ©sitation que la rÃ©ponse est non.Â Â»*

Sources :

- Â« Covid-19 : la vie privÃ©e sera-t-elle une victime collatÃ©rale de l'Ã©pidÃ©mie de coronavirus ? Â», Fabien Soyez, cnetfrance.fr, 10 avril 2020.
- Â« Covid-19 : Bluetooth, serveur central, logiciel libreâ€¦ On en sait un peu plus sur StopCovid Â», Alice Vitard, usine-digitale.fr, 20 avril 2020.
- Â« Entre Bubble et Apollo, la petite histoire du traÃ§age commun d'Apple et de Google Â», MickaÃ«l Bazoge, igen.fr, 28 avril 2020.
- Â« Application StopCovid : la France isolÃ©e dans son bras de fer avec Apple et Google Â», Damien Leloup,Â *Le Monde*, 28 avril 2020.
- Â« Recours aux Gafam, centralisation : les choix techniques sur StopCovid ont attisÃ© les tensions au sein de lâ€™Ã‰tat Â», Ã‰mile Marzolf, acteurspublics.fr, 30 avril 2020.
- Â« StopCovid ou encore ? Â» Cedric 0, medium.com, 3 mai 2020.
- Â« CentralisÃ© ou dÃ©centralisÃ© : quelles diffÃ©rences entre les architectures des apps de contact tracing ? Â», FranÃ§ois Manens, numerama.com, 5 mai 2020.
- Â« StopCovid, toutes les rÃ©ponses Ã vos questions sur lâ€™application du dÃ©confinement Â», frandroid.com, 7 mai 2020.
- Â« DÃ©libÃ©ration nÂ° 2020-056 du 25 mai 2020 portant avis sur un projet de dÃ©cret relatif Ã lâ€™application mobile dÃ©nommÃ©e Â« StopCovid Â» (demande dâ€™avis nÂ° 20008032) Â», cnil.fr, 25 mai 2020. Â« StopCovid : l'INRIA va remplacer l'algorithme de chiffrement de l'application de contact tracing Â», StÃ©phane le Calme, developpez.com, 25 mai 2020.
- Â« Dans quel cas lâ€™app StopCovid sera-t-elle efficace ? Â», Marie Turcan, numerama.com, 27 mai 2020.
- Â« Application StopCovid : que sait-on du projet franÃ§ais de traÃ§age des contacts ? Â», Julien Lausson, numerama.com, 28 mai 2020.
- Â« Application StopCovid : accouchÃ©e dans la douleur, et une efficacitÃ© dÃ©jÃ remise en

cause Â», Sylvain Tronchet, franceinter.fr, 30 mai 2020.
- Â« FAQ sur les aspects techniques de l'application StopCovid Â», inria.fr, 1er juin 2020.
- Â« StopCovid demande lâ€™accÃ¨s Ã la gÃ©olocalisation sur Android, mais sâ€™engage Ã ne pas lâ€™utiliser Â», Julien Lausson, numerama.com, 2 juin 2020.
- Â« Too much contact data sent to the server Â», GaÃ«tan Leurent, GitLab, Inria.fr, June 12, 2020.
- Â« StopCovid, lâ€™appli qui en savait trop Â», GÃ©raldine Delacroix, mediapart.fr, 15 juin 2020.
- Â« Lâ€™application StopCovid collecte plus de donnÃ©es quâ€™annoncÃ© Â», *Le Monde*, 16 juin 2020.Â

Categorie

1. Techniques

date crÃ©Ã©e
18 juillet 2020
Auteur
jacquesandrefines