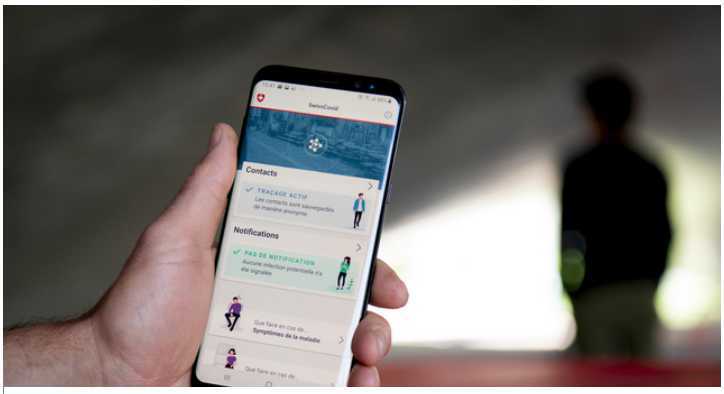
SANTÉ | **CONTACT TRACING** | ENQUÊTE
Publié le 08 juin 2020, 18:45. Modifié le 09 juin 2020, 10:44.

EXCLUSIF - Une analyse de l'EPFL met en garde contre les failles de SwissCovid

par Annick Chevillot



SwissCovid, l'application de contact tracing de l'EPFL et l'ETHZ, a été validée par le Parlement. | Keystone / Laurent Gilliéron

Alors que le Conseil national a approuvé ce 8 juin la base légale permettant de lancer publiquement l'application de *contact tracing* SwissCovid d'ici la fin du mois de juin, des voix s'élèvent pour mettre en garde sa sécurité, ses protocoles de mises en service et leur transparence. Ces critiques n'émanent pas que de la société civile et de responsables des protections des données, mais également de l'EPFL et de l'Université de Lausanne. Mais quels risques court-on vraiment à la télécharger?

Pourquoi c'est déroutant. Les conseillers aux Etats ont adopté à une large majorité mercredi 3 juin la loi autorisant le déploiement de SwissCovid au niveau national. Ce lundi, c'était au tour des conseilleurs nationaux de se prononcer. Leur acceptation a été une formalité (156 voix pour, 22 contre et 13 abstentions). Mais ont-ils pris leur décision en toute connaissance de cause? Une analyse – pas encore publique, mais que *Heidi.news* a pu se procurer –

issue du Laboratoire de sécurité et de cryptographie (Lasec) de l'EPFL met en garde contre les abus possibles et le manque de transparence qui a prévalu dans le processus de développement, alors même que les chercheurs des écoles polytechniques fédérales impliqués dans le projet ont organisé un webinaire sur le sujet le 27 mai. Enquête.

De quoi on parle. L'application SwissCovid se base sur un protocole dit DP-3T, pour *decentralized privacy preserving proximity tracing*. C'est un consortium d'experts internationaux qui l'a dévelopée, dont des chercheurs de l'EPFL et de l'ETHZ.

Le but: contrôler l'évolution de l'épidémie en informant les utilisateurs lorsqu'ils ont été en contact étroit avec une personne infectée, pour qu'ils puissent se placer en quarantaine si nécessaire. L'ensemble fonctionne notamment grâce au signal Bluetooth émis par les smartphones. Ce protocole informatique permet de détecter si un autre utilisateur se trouve et s'est trouvé à une distance suffisamment proche (un à deux mètres) pour transmettre le coronavirus.

Depuis, le début du projet, d'autres partenaires sont entrés dans le processus: Google, Apple et Amazon, notamment. Les deux premiers pour assurer un déploiement maximal de l'application sur les smartphones Android et iOS, le dernier pour ses serveurs. Cette évolution, transparente bien qu'assez discrète, fait craindre des problèmes de sécurité et de protection des données. De plus, le code source hébergé sur GitHub en open source pose problème à certains détracteurs, qui argue du fait que GitHub appartient à Microsoft. Ces éléments permettent de mettre au jour des failles potentielles et aussi de développer un argumentaire idéologique contre SwissCovid.

Les promesses. SwissCovid se veut efficace et respectueuse des données de ses utilisateurs.

L'application se veut sécurisante, transparente, innovante, digne de confiance, anonyme et fait appel à la responsabilité individuelle:

La transparence. Ce point est crucial pour obtenir l'adhésion de la population. Des efforts de communication importants ont été menés, notamment par l'EPFL, pour expliquer encore et encore l'utilité du dispositif. Des tests d'intrusion ont été menés par des spécialistes de la sécurité informatique. Les failles ainsi découvertes sont signalées publiquement à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani). Cette procédure permet de corriger et d'améliorer l'application. Il est possible de consulter ce développement, assez technique, sur la page internet où le DP-3T est documenté, sur GitHub.

Les critiques. Pour les détracteurs de SwissCovid, tout n'est pas aussi rose. Auteur de nombreux posts sur les réseaux sociaux et d'avis sur la question, Sébastien Fanti, avocat et préposé valaisan à la protection des données et à la transparence, a très vite alerté sur les risques d'une telle application:

> «Qui a audité ce dispositif? Je veux dire qui n'était pas partie prenante à l'élaboration de l'application? Cela manque, clairement. La Confédération n'est pas non plus très transparente dans l'évolution du projet. L'Etat a été très discret sur l'implication de Google, Apple et Amazon. C'est pourtant central pour un tel outil qui s'apparente à un dispositif médical et doit donc être soumis au secret médical. Quels contrats ont été signés avec ces

> trois entreprises? Quelle en est la teneur? A quoi la Confédération s'est engagée avec ses contrats? J'attends toujours les réponses à ces questions.
>
> Comprenez-moi bien, je n'ai rien contre le traçage, mais pour être sûr que cela fonctionne, il était nécessaire de créer une commission d'experts indépendante. Ce qui n'a pas été fait. Il faut susciter un débat public sur cette question, exposer des avis pour et contre. Je constate simplement que le débat démocratique n'est pas possible avec les porteurs du projet, qui doit être sécurisé. Un exemple: si un problème devait survenir, il n'y a pas de clause de responsabilité clairement établie. J'aimerais bien savoir quelle est l'ampleur du risque à utiliser SwissCovid.»

Du côté de l'Université de Lausanne (Unil), c'est la Pre Solange Ghernaouti, directrice du Swiss cybersecurity Advisory & Research Group (SCARG), qui a évoqué les problèmes de sécurité de SwissCovid, notamment sur son blog du *Temps*. Les questions qu'elle y pose et ses avis mélangent opinions et failles techniques potentielles, sans être forcément avérées sur le terrain. Contactée, elle détaille les problèmes de sécurité qu'elle a relevé:

> **Bluetooth:** «Il existe des attaques bien connues qui exploitent la nature même du canal de transmission: l'échange de données Bluetooth sur ondes hertziennes, indépendamment de la finalité des échanges ou de l'application qui utilise Bluetooth. On peut citer: captation, interception par un tiers non autorisé des messages transmis sur l'interface Bluetooth; insertion, suppression de messages par un tiers; observation des signaux (écoute, espionnage); interruption de la connectivité (déni de service); prise de contrôle à distance.»

Développement: «Il est relativement facile de développer un système personnel de surveillance; de générer des fausses alertes (de cibler certaines personnes, certaines entreprises, certains secteurs d'activité); de connaitre où et quand se trouvent les utilisateurs. Ainsi, rien n'interdit un utilisateur d'enregistrer régulièrement ses coordonnées de géolocalisation. Il pourra ainsi savoir à quelle heure et où il se trouvait lorsqu'il est susceptible d'avoir été exposé. Dans certaines conditions, il peut donc savoir par qui.»

Problèmes non-résolus: «Comment lever la contradiction majeure entre le besoin de sécurité informatique et l'impérieuse nécessité de SwissCovid que la fonctionnalité Bluetooth du téléphone soit toujours active? Comment s'assurer que les failles ne sont pas exploitées? Comment s'assurer que les environnements des utilisateurs sont bien séparés, étanches et sécurisés (application et données de traçage, données personnelles, données financières, paiement en ligne, etc.)? Comment s'assurer qu'il y a bien étanchéité entre l'application de traçage et la plateforme d'exécution (smartphone, applications constructeurs)?»

Un pseudo-anonymat: «La responsabilité des défauts de sécurité est portée par l'utilisateur final, alors qu'il n'a pas les moyens et la compétence de s'assurer que toutes les failles de sécurité sont bien identifiées et réparées, que les bugs (défauts techniques) ne sont pas exploités, et que la protection des données personnelles et de l'intimité numérique (privacy) est bien effective. Dans la mesure ou le processus de génération des pseudonymes est un des piliers de l'application, il est nécessaire de s'assurer que le processus ne peut pas être compromis. A ce jour, il n'y a pas d'assurance. Il s'agit de pseudo-anonymat, pas d'anonymat!»

Identifiants: «Il est impossible de garantir qu'à partir des identifiants pseudos générés, il ne soit pas possible de remonter à l'identification de la personne, que les pseudos ne puissent être associés aux divers identifiants de la personne et du téléphone (Imsi, Imei, numéro de téléphone, compte, etc.). Le chaînage et le recoupement d'informations est possible. Sur Android, pour télécharger l'application, l'utilisateur doit avoir un compte Gmail (Google). Il y a donc association entre un compte et un équipement.»

Absence de garanties: «À ce jour, on ne peut pas garantir que les données ayant fait l'objet d'une pseudo-anonymisation, ne permettent pas d'identifier des personnes (notamment par recoupement d'information, croisement des données, déduction, profilage des contacts, etc.). On ne peut pas garantir non plus que le système ne soit pas détourné: qu'un téléphone dédié spécialement soit utilisé à proximité d'une personne ciblée pour être alerté si cette personne est déclarée positive. Cette possibilité de détournement ne nécessite pas de compétence particulière.»

Stigmatisation: «Nous n'avons également aucune garantie que ce type de dispositif ne permet pas de constituer des fichiers de personnes malades et engendre des dérives potentielles importantes, ni que le système de traçage ne se transforme en système de dénonciation, en système de stigmatisation des malades ou des personnes porteuses asymptomatiques. On peut même imaginer que le système devienne la base d'un système discriminatoire d'octroi de prestation, d'accès à des services, lieux, institutions, etc. Et… le système de traçage pourrait-il contribuer à transformer la contamination involontaire en faute?»

Pour Solange Ghernaouti,

> «À moins de considérer les futurs utilisateurs comme des cobayes pour améliorer la solution, le temps des tests et des certifications indépendantes (sans conflit d'intérêt) – pour ne pas s'appuyer uniquement sur les auto-déclarations des concepteurs – il est nécessaire que le système fasse l'objet de procédés d'audibilité et de vérifiabilité par des entités indépendantes. Il est demandé, avant de déployer SwissCovid, d'avoir la possibilité de faire des tests de sécurité de la version finale de SwissCovid, comme ce fut le cas pour l'e-voting.»

Du côté de l'EPFL, c'est le Pr Serge Vaudenay, du Laboratoire de sécurité et de cryptographie (Lasec), qui a rédigé une analyse critique sur SwissCovid. Elle a été soumise à Melani le 5 juin mais n'est pas publique pour des raisons de réglementation. *Heidi.news* a toutefois pu se la procurer et s'entretenir avec Serge Vaudenay sur le sujet. Selon cette analyse, SwissCovid crée des menaces critiques pour la sécurité et la vie privée. Qu'elles soient réduites ou non, elles doivent être communiquées. Plus important encore, il est nécessaire de communiquer que:

> les informations disponibles sont insuffisantes,
>
> il existe des idées fausses sur l'anonymat et l'open source,
>
> il ne semble pas y avoir de place pour le test de sécurité publique dans l'agenda,
>
> les développeurs de SwissCovid sont liés aux décisions de Google et Apple.

Serge Vaudenay:

> «Les parlementaires qui se sont prononcés sur la base légale pour lancer l'application

> SwissCovid n'ont pas connaissance des problèmes relevés dans l'analyse soumise le 5 juin. Ils n'en auront pas connaissance avant d'avoir voté et c'est regrettable. Je ne fais pas partie de l'équipe de développement, je suis juste un testeur qui identifie les failles et les signale. Il en existe plusieurs, connues mais non documentées. Un autre problème est que la majeure partie du protocole est installé sur les
> téléphones utilisant Android et iOS, indépendamment de SwissCovid. Cette application sert finalement juste d'interface entre utilisateurs, serveurs et cette partie déjà présente.
>
> Ce n'est pas un problème de sécurité en soi, mais comme il n'est pas possible d'avoir accès aux codes source de Google et d'Apple, il n'est pas possible de dire qu'on a affaire à une application open source. A ce stade, il n'est pas possible de vérifier que le code source correspond à ce qui est mis à disposition sur GitHub. De plus, il existe une confusion concernant les clefs supposées anonymes (*elles permettent d'envoyer les notifications aux utilisateurs ayant été en contact avec une personne testée positive, ndlr)*: il ne s'agit pas d'anonymat, mais de pseudonyme. Ces clefs sont liées aux utilisateurs et devraient être liées au secret médical, alors que le protocole de SwissCovid suppose que ces données seront publiques.»

Pour le spécialiste, ce qui manque le plus, c'est la phase de tests publics et l'absence de documentation concernant l'implémentation et la configuration du code source sur les serveurs Amazon — «on doit les deviner», souligne-t-il.

Pour le chercheur, les échanges avec l'équipe qui conçoit l'application à l'EPFL sont limités. Selon nos

sources, les discussions seraient même musclées. Et de lancer une analogie:

> «On était censé aller aussi vite que possible et aussi lentement que nécessaire. Mais avec SwissCovid, on est juste allé trop vite.»

Le fond du problème. SwissCovid représente une véritable innovation technologique, avec toutes les difficultés relevées ci-dessus. En révélant ses imperfections, ses contradicteurs permettent de l'améliorer.

Le problème est donc aussi et surtout idéologique et politique. Ainsi, ce n'est pas parce que GitHub appartient à Microsoft que l'on peut pour autant conclure que le code source de l'application n'est pas en open source. On ne peut pas non plus partir du principe que parce que Google, Apple et Amazon donnent accès à des services, qu'on est confronté à une application liberticide ou que l'on est face à une «GestapoApp», comme le soulignait le 1er juin le conseiller national valaisan (UDC), Jean-Luc Addor, sur Twitter:

En tant que citoyenne confrontée comme tout
blogs.letemps.ch

1 22:47 - 1 juin 2020

Voir les autres Tweets de Jean-Luc Addor

Il aurait été difficile d'atteindre un taux de pénétration suffisant sans s'associer à Google et à Apple. Pour ce qui est d'Amazon, Anouch Seydtaghia, expliquait dans *Le Temps* le 4 juin dernier que l'entreprise dispose de «ressources informatiques qui n'existent pas en Suisse, comme le suggère un porte-parole de l'Office fédéral de la santé publique (OFSP): «Le système de récupération des clés des personnes infectées est géré par l'Office fédéral de l'informatique et de la télécommunication (OFIT), mais utilise – en accord avec le préposé fédéral à la protection des données – le système Cloudfront d'Amazon pour la distribution du contenu. En effet, les volumes de données à traiter nécessitent un réseau de distribution de contenu fourni par un tiers.»

Du côté de l'EPFL, on assure qu'il n'existe aucun moyen de connecter ces clés aux utilisateurs. Le travail critique et étayé de Serge Vaudenay est salué par plusieurs experts, internes et externes à l'école polytechnique, parce qu'il permet de corriger l'application. Selon nos sources au sein de l'EPFL *(qui désirent demeurer anonymes, ndlr)*, il est nécessaire que les failles de sécurité soient identifiées. Ce travail d'analyse est donc perçu comme une chance d'amélioration.

A l'inverse, certaines voix à l'EPFL s'inquiètent que ces critiques, légitimes mais mineures, ne soient instrumentalisées par les tenants de théories du complot. Ou sorties de leur contexte pour critiquer l'appli en négligeant l'enjeu majeur de santé

publique: participer à l'endiguement de l'épidémie jusqu'au 30 juin 2022, date d'échéance de cette loi.

Les politiques pragmatiques. Les conseillers aux Etats ont plébiscité la loi permettant le déploiement de SwissCovid. Les conseillers nationaux l'ont également approuvé ce jour. Au Parlement, l'application n'a soulevé que peu de débats, à peine quelques questions. Des critiques ont été essentiellement émises dans les rangs des Verts et de l'UDC. Mais la plupart se sont montrés pragmatiques. A l'image de Damien Cottier, conseiller national neuchâtelois (PLR):

> «Le Parlement s'est assuré d'obtenir des garanties de sécurité. Garanties qui seront inscrites dans une base légale et devront donc être impérativement respectées. J'ai confiance en notre gouvernement et rien ne m'induit à penser que ces garanties ne seraient pas respectées.
>
> Cela dit, le risque zéro n'existe évidemment pas, mais la possibilité qu'une personne soit identifiée ou que ses contacts soient reconstruits par des personnes mal intentionnées a été ramené au minimum et l'on peut affirmer qu'à ce stade, les risques sont à un niveau si bas qu'ils sont parfaitement acceptables et tout à fait proportionnés. Quand au risque d'être traqué par une autorité publique, il est exclu. En fait cette application est certainement beaucoup plus sûre que la plupart des programmes ou applications que des millions de personnes utilisent au quotidien. C'était important d'y veiller car SwissCovid est éditée et recommandée par une autorité publique dans un domaine particulièrement sensible, celui de la santé.»

De nombreux politiciens rencontrés à Berne ce lundi 8 juin partagent l'avis que SwissCovid représente un complément utile au travail de traçage des contacts

mené par les cantons. Et selon un sondage de la RTS, deux tiers des élus fédéraux comptent installer l'app de traçage SwissCovid. Damien Cottier:

> «Pour ma part, je la téléchargerai dès qu'elle sera disponible après la phase test. La Suisse est pionnière mondiale en la matière. Nous avons une app sûre, respectueuse des données de chacun et qui peut se montrer très utile. Plus il y aura d'utilisateurs, plus son utilité va augmenter. S'il y a un pays au monde où l'on peut utiliser cette app en toute sécurité, c'est bien la Suisse!»

Un choix personnel. Au final, SwissCovid a encore besoin de répondre aux critiques soulevées et tenir ses promesses pour rassurer pleinement la population. L'expert genevois en cybersécurité Stéphane Koch se veut rassurant:

> «Un climat de peur s'installe autour de SwissCovid. Pourtant, le risque avec cette application est infime, par rapport à d'autres app que l'on utilise au quotidien. Ce n'est pas la peur qui doit empêcher les gens de l'utiliser. Il y a un intérêt à savoir qui a été en contact avec des personnes testées positives. Personnellement, je n'ai pas envie d'infecter d'autres personnes! C'est bien d'avoir mis en place un outil qui aide à lutter contre l'épidémie.»

Parlement **Covid-19** **Coronavirus** **Déconfinement** **Contact Tracing**