SwissCovid sous le feu des critiques: quatre questions pour comprendre

**TECHNOLOGIE**

Encore en phase de test, l’application de traçage de contacts est l’objet de vives critiques, tant à cause de l’implication de multinationales américaines qu’à propos de son niveau de sécurité. Voici quatre points pour se faire une opinion

[Anouch Seydtaghia](https://www.letemps.ch/auteur/110)

Publié mercredi 10 juin 2020 à 18:44
Modifié mercredi 10 juin 2020 à 22:29

* [**8**](https://www.letemps.ch/economie/swisscovid-feu-critiques-quatre-questions-comprendre?utm_source=Newsletters&utm_campaign=2d81d25d4b-newsletter_briefing&utm_medium=email&utm_term=0_56c41a402e-2d81d25d4b-109968281#commentaires)

«C’est une application sous le contrôle de Google, Amazon, Apple et Microsoft.» «Elle comporte plusieurs failles de sécurité.» Et «son code source est inaccessible». Voilà, en trois phrases, une synthèse des vives critiques qui s’abattent depuis quelques jours sur SwissCovid, l’application de traçage des contacts destinée à lutter contre la propagation du virus. Avant son lancement officiel, prévu d’ici à la fin du mois de juin, *Le Temps* s’est intéressé à ces critiques, diffusées principalement via les réseaux sociaux. Avec l’objectif de démêler le vrai du faux, SwissCovid suscitant bien des fantasmes.

**1. Quel rôle joue Amazon?**

La «suissitude» de l’application avait été présentée comme un atout majeur de l’app par l’EPFL et l’Office fédéral de la santé publique (OFSP). Mais le 3 juin, une petite phrase, prononcée par le conseiller aux Etats (SG/PS) Paul Rechsteiner, a mis le feu aux poudres. «Il y a une coopération avec Amazon Allemagne à Francfort pour l’examen des contacts», a dit le parlementaire en préambule à un débat.

La multinationale américaine examinerait-elle les données des Suisses, qui plus est dans un centre basé à l’étranger? En réalité, aucun de ces deux points n’est correct. La seule chose qui est exacte, c’est qu’un des services d’Amazon est utilisé, plus précisément son réseau de distribution de contenu (Content Delivery Network, ou CDN). Celui-ci permet de diffuser les clés – une suite aléatoire de chiffres et de lettres –, qui sont les identifiants anonymes et générés aléatoirement pour chaque utilisateur de SwissCovid. Le CDN d’Amazon se charge de mettre ces clés à la disposition des téléphones lorsqu’une personne se déclare infectée par le virus.

Comme le précise Edouard Bugnion, vice-président de l’EPFL, «aucun calcul et aucune analyse n’a lieu chez Amazon. Les données diffusées par le CDN sont générées par des serveurs qui se trouvent dans le canton de Berne, dans des centres de calcul de la Confédération, gérés par l’Office fédéral de l’informatique et de la télécommunication. Ces serveurs de la Confédération signent cryptographiquement les données avant leur diffusion.»

Mais pourquoi faire appel à Amazon pour un service qui pourrait, a priori, être effectué par un prestataire suisse? Edouard Bugnion répond que «les CDN sont une composante essentielle d’internet et nécessitent une infrastructure mondiale. La Confédération utilise depuis plusieurs années le service CloudFront d’Amazon, alors que par exemple l’EPFL emploie les services d’un autre CDN et votre journal un troisième. Les trois sont américains.»

**Lire aussi:** [Pourquoi SwissCovid doit utiliser les services d’Amazon en Allemagne](https://www.letemps.ch/economie/swisscovid-utiliser-services-damazon-allemagne)

**2. L’application est-elle sûre?**

Mardi, le préposé valaisan à la protection des données et à la transparence publiait un communiqué concernant SwissCovid. Dans celui-ci Sébastien Fanti recommandait aux collaboratrices et collaborateurs de l’administration cantonale de ne pas télécharger la version pilote SwissCovid. Le préposé cantonal citait un rapport d’experts de l’EPFL indiquant que «l’application SwissCovid qui se trouve au stade de projet présentait des failles importantes en termes de privacité et de sécurité. Ainsi, sur le plan technique, les experts de la même Ecole polytechnique fédérale sont divisés sur des questions fondamentales, ce qui doit engendrer l’application du principe de précaution.»

Ce rapport d’experts a notamment été signé par Serge Vaudenay, professeur en cryptographie de l’EPFL. Dans ce document de 25 pages, il cite tout une série d’attaques que pourrait subir SwissCovid et regrette qu’il n’y ait pas assez de temps pour qu’un audit public soit mis en place pour tester l’application. Edouard Bugnion réplique en affirmant qu’«une liste détaillée des attaques que pourrait subir l’application a été documentée depuis longtemps par nos soins. Cela dit, nous tenons compte de toutes les critiques et remarques et améliorons sans cesse l’app durant la phase pilote.»

Certaines affirmations contenues dans ce rapport sont jugées incorrectes par l’EPFL. Ainsi, il y est écrit que «le serveur est hébergé par Amazon», ce qui est clairement démenti par la vice-présidence de l’école.

**Lire aussi:** [Avant le feu vert officiel, SwissCovid a été téléchargée plus de 50 000 fois](https://www.letemps.ch/economie/feu-vert-officiel-swisscovid-telechargee-plus-50-000)

**3. Le code source de l’app est-il accessible?**

C’est une question importante qui a directement un lien avec le point précédent. Dès le début – et ce point est d’ailleurs clairement stipulé dans le projet de loi en cours d’acceptation par le parlement –, l’EPFL a affirmé que le code source serait accessible à tous. Cela permet un audit public, une pratique habituelle pour améliorer la sécurité d’un programme.

Plusieurs critiques affirment que le code source de SwissCovid n’est pas disponible. C’est totalement faux, affirme Edouard Bugnion. «Le code de l’application est accessible sans aucune restriction contractuelle, et sous une licence open source très communément utilisée.» Le vice-président de l’EPFL précise que «le code source est disponible depuis le début sur Github. Il permet notamment de vérifier que SwissCovid ne contient pas de fonctionnalités non essentielles pour l’exécution de l’app». GitHub est une plateforme de créations de logiciels, acquise en 2018 par Microsoft. Mais aucune interférence entre la firme américaine et le contenu publié sur GitHub n’a été signalée.

**4. Une dépendance trop forte à Apple et Google?**

Certains estiment que l’app est trop dépendante des systèmes d’exploitation pour mobiles mis à jour par Apple et Google. «Nous avons effectivement tous une dépendance numérique qui démarre lors de l’achat de nos téléphones avec l’un ou l’autre des deux seuls systèmes d’exploitation du marché. Cela dit, il faut nuancer dans le cas de SwissCovid», affirme Edouard Bugnion. Il poursuit: «SwissCovid est responsable de toutes les interactions avec les serveurs de l’OFSP, de la validation des COVIDcode et de l’ensemble des paramètres du modèle épidémiologique choisis par l’OFSP. Par contre, les échanges Bluetooth sont gérés par les systèmes d’exploitation dont nous n’avons pas le code source, mais une documentation précise. Ce support à l’intérieur des systèmes d’exploitation améliore les performances, les calibrations entre différents modèles de téléphones, et l’interopérabilité à l’international. En plus, il impose le modèle décentralisé que nous préconisons depuis le début car il garantit la non-exploitation centralisée (en particulier par un Etat) des données de proximité récoltées par les téléphones.»

PUBLICITÉ

Autres articles sur le thème [Technologies](https://www.letemps.ch/theme/technologies)

Vos contributions

* [Choix rédaction (0)](https://www.letemps.ch/economie/swisscovid-feu-critiques-quatre-questions-comprendre?utm_source=Newsletters&utm_campaign=2d81d25d4b-newsletter_briefing&utm_medium=email&utm_term=0_56c41a402e-2d81d25d4b-109968281#my-content-favorites)
* [Toutes les contributions (8)](https://www.letemps.ch/economie/swisscovid-feu-critiques-quatre-questions-comprendre?utm_source=Newsletters&utm_campaign=2d81d25d4b-newsletter_briefing&utm_medium=email&utm_term=0_56c41a402e-2d81d25d4b-109968281#my-content-favorites)

André L.

Il y a 22 heures

Sur le rôle d'Amazon (première question), pourquoi les EPF n'ont-elles pas fait appel à un réseau de diffusion de contenu (content delivery network) suisse? Par exemple, la SRG SSR utilise les services de SWISS TXT (<https://www.swisstxt.ch/en/cases/cdn-manager/>). Il existe au moins quatre de ces réseaux à Zurich.

Au sujet de la sécurité (deuxième question), selon Edouard Bugnion «une liste détaillée des attaques que pourrait subir l’application a été documentée depuis longtemps par nos soins." Si le vice-président de l'EPFL se réfère à la liste des menaces décrites dans le "white paper" (livre blanc) du projet COVID, celles-ci y sont en effet décrites en détail et doivent être lues avec la plus grande attention. Certaines font même froid dans le dos. Pourtant, aucune contre-mesure n'est proposée contre ces menaces.

Quant aux failles de Bluetooth, elles sont connues pour avoir déjà affecté des milliards de mobiles, comme l'a rapporté le CNET (France): "BlueBorne : 8 failles dans le protocole Bluetooth, des milliards d’appareils touchés” - [https://www.cnetfrance.fr/news/blueborne-8-failles-dans-le-protocole-bl…](https://www.cnetfrance.fr/news/blueborne-8-failles-dans-le-protocole-bluetooth-des-milliards-d-appareils-touches-39857326.htm)).

Sur l'accès au code source (troisième question) - toujours selon Edouard Bugnion -, il "est accessible sans aucune restriction contractuelle, et sous une licence open source très communément utilisée." M. Bugnion précise que «le code source est disponible depuis le début sur Github".

Pourtant, ce que le vice-président de l'EPFL ne dit pas, c'est que la licence MPL (Mozilla Public License) 2.0, utilisée pour l'application, permet au contraire d’autres licences libres (par exemple, de GPL), de combiner des fichiers sous licence MPL et sous une autre licence (propriétaire ou non) dans un même logiciel, et seules les modifications apportées aux fichiers sous licence MPL doivent être publiées sous cette licence. Si les modifications d’un fichier sous MPL doivent être rendues publiques, ce n’est pas forcément le cas de ces autres fichiers adjoints au programme.

De plus, M. Bugnon affirme qu'aucune interférence entre la firme américaine Microsoft, propriétaire de GitHub, sur le site duquel le code et la documentation de l'application sont disponibles, n’a été signalée. Or, peut-on sérieusement inférer que la majorité des utilisateurs sera en mesure de télécharger, installer et exécuter, sans même parler de le modifier, le code dans son intégralité sur son android ou son ios? Il n'est déjà pas évident d'y installer Bluetooth. Peut-on dès lors attendre de l'utilisateur lambda qu'il construise une telle application avec "gradlew", soit en ligne de commande, ce qui suppose une connaissance au moins élémentaire du langage java, soit avec une version récente d'Android? Sous le prétexte d'être rendus publics, le code et la documentation disponibles en ligne ne s'adressent-ils pas en réalité d'abord, sinon aux spécialistes, du moins aux amateurs avertis?

Enfin, au sujet de la dépendance à Google et Apple (quatrième question), comment peut-on affirmer que le code est en source libre quand il dépend d'android (propriété de Google) et d'ios (Apple) et ne peut être construit et exécuté sans ces logiciels commerciaux?

Les affirmations du vice-président de l'EPFL ne soulèvent-elles pas plus de questions qu'elles n'apportent de réponses?

Luc B.

Il y a 20 heures

@André L.
SwissTxt est un partneraire Akamai et utilise donc aussi un CDN externe.

Les attaques citées demandent un investissement non négligeable et sont inhérentes à du contact tracing. Je vous invite toujours à comparer celà à du contact tracing fait manuellement où vous devez donner le nom et les lieux visités...

Si vous n'utilisez jamais le Bluetooth, tant mieux pour vous. Fait est que la plupart des gens ont reçu des mises à jours et utilisent le Bluetooth. Si par hasard, les quelques personnes qui n'utilisent pas le BT à cause de ces failles n'utilisent pas SwissCovid, ce sera de loin pas un drame.

Le code est open source non pas pour que chacun puise compiler l'application lui-même, mais que ceux qui le désirent puissent le faire et ainsi étendre la confiance non pas seulement au développeur originaux.

Si vous ne faites pas confiances à Google / Apple, j'espère que vous vous tenez à votre ligne et que vous n'utiliser ni appareil iOS/Android. Dans ce cas, SwissCovid ne sera de toute manière pas pour vous. Les 99% autres pourcents de la population se feront par contre un plaisir de sauver des vies grâce à leur smartphone!

Lucas S.

Il y a 10 heures

Pourquoi appelle-t-on des "clés" les codes diffusés par le CDN d'Amazon et non pas simplement des identifiants d'utilisateurs? Que permettent-elles de déchiffrer pour mériter l'appellation "clé" ?

Suzanne B.

Il y a 9 heures

Entièrement d'accord avec Luc B.
Ceux qui ont peur de l'application SwissCovid devrait commencer par être conséquents et ne pas utiliser de téléphone portable du tout. Mais je suis sûre qu'on trouverait Whatsapp, la recherche par Google, et bien d'autres applications bien moins sûres et nettement plus "poreuses" que SwissCovid sur leur portable!

Louis B.

Il y a 9 heures

@Lucas S.
Du fait du protocole DP³T qui est au cœur de SwissCovid, il s'agit vraiment de clefs au sens cryptographique du terme. Ces clefs permettent de reconstituer les codes éphémères que l'utilisateur a généré pendant qu'il était asymptomatique. Je note que, contrairement à l'utilisation habituelle des clefs cryptographiques, ces données doivent être rendues largement accessibles dans ce scénario puisqu'elles sont nécessaires pour déclencher des alertes d'exposition. Au passage, c'est cela qui justifie à mon sens l'usage d'un CDN.

Hubert G.

Il y a 9 heures

Les failles bluetooth mentionnées sur le site CNET sont vieilles (2017) et ont été corrigées depuis longtemps !!!
Quant à la dépendance vis-à-vis de Google/Apple, je me permets de rappeler que la plupart des logiciels utilisés sur la planète reposent sur les plateformes des GAFAMi (+IBM) , y compris les infrastructures très sensibles.
Même le super ordinateur de l'EPFL a été piraté ...
Ces points mettent en lumière une fois de plus les vulnérabilités de nos activités au quotidien , pas seulement une petite application bien marginale .

Giovanni C.

Il y a 5 heures

Article ridicule, écrit sans même pas prendre la peine de vérifier les informations sur lesquelles il se pose.
Il faut areter de diffuser des articles dont le seul but est celui de attirer des click sur les social networks (leur oui respectueux de la privacy!)
Le code source de l'application est disponible sur github dupuis le tout premier jour. Les concepteurs ont tout donné pour nous fournir une application la plus respectueuse de notre vie privé que possible et dans des délais très courts.
Les librairies mis à disposition par google et apple sont la pour aider les developper à aller plus vite car gagner du temps dans cet cas signifie éviter des mort. Cette collaboration entre les deux acteurs majeur du marché des smartphones est première mondial que il faudrait saluer comme une grand succès de l’EPFL.
En publiant des articles comme cela vous assumez la responsabilité des souffrances et des décès car il y aura des personnes qui ne vont pas installer l’application pour craint de perdre leur privacy quand les 8 web trackers présentes dans votre site leur auront fait perdre 1000 fois plus de privacy que l’application swisscovid!

Jean-Marc R.

Il y a 4 heures

De mon côté, le défaut majeur de l'application est qu'elle n'est compatible qu'avec la version la plus récente d'IOS (13.5) pour les iPhone d'Apple. Pour ceux, encore très nombreux, qui utilisent une version antérieure, l'application ne sera pas disponible. Cette limitation malheureuse est incompréhensible car elle va directement à l'encontre de l'objectif de SwissCovid.