L'application StopCovid autorisée pour six mois maximum après la fin de l'état d'urgence sanitaire

Le traitement de données StopCovid est créé par un décret du 29/05/2020, publié au Journal officiel du 30/05. Relatif à l'application StopCovid développée par une équipe-projet pilotée par Inria, ce traitement est sous la responsabilité de la direction générale de la santé du ministère des solidarités et de la santé.

Le premier objectif de ce dispositif, selon le décret, est « d'informer les personnes utilisatrices de l'application qu'il existe un risque qu'elles aient été contaminées par le virus du Covid-19 en raison du fait qu'elles se sont trouvées à proximité d'un autre utilisateur de cette application ayant été diagnostiqué positif à cette pathologie ».

Les critères définissant un contact conservé par StopCovid sont définis par un arrêté du 30/05, publié au Journal officiel du 31/05 : les téléphones de deux utilisateurs de l'application doivent être à moins d'un mètre pendant au moins 15 minutes.

StopCovid est mis en œuvre pour une durée ne pouvant excéder six mois après la cessation de l'état d'urgence sanitaire, précise le décret. La DGS devra rendre public un rapport sur le fonctionnement de StopCovid dans les trente jours suivant le terme de la mise en œuvre de l'application, et au plus tard le 30/01/2021.

Ces deux textes sont publiés au Journal officiel après que le gouvernement a fait une déclaration au Parlement sur le sujet, le 27/05. Cette déclaration a été suivie d'un débat et approuvée par un vote dans chacune des deux chambres.

L'application est téléchargeable, depuis le 02/06, sur l'Apple Store et sur Google Play.

Publication du code source de StopCovid : engagements du décret et enjeux

« Le code source mis en œuvre dans le cadre de StopCovid est rendu public et est accessible à partir des sites internet du ministre des solidarités et de la santé et du ministre de l'économie et des finances ainsi que du site internet www.stopcovid.gouv.fr », indique par ailleurs le décret.

Un point sur lequel la Cnil avait insisté, dans son avis du 25/05/2020, publié le 26/05 :

> *« Concernant la publication du code source, le projet de décret mentionne que certains éléments du "code informatique" de l'application ou du serveur central ne seront pas rendus publics, car cela mettrait en danger l'intégrité et la sécurité de l'application. Même si le paramétrage des logiciels utilisés et le détail des mesures de sécurité n'ont pas vocation à être rendus publics, il est important que l'intégralité du code source soit quant à lui rendu public.*
>
> *La commission accueille favorablement l'engagement du ministère de rendre public l'intégralité du code source et suggère que le décret soit modifié en conséquence. »*

De son côté, Inria annonçait le 12/05 commencer la publication du code source et de la documentation de l'application, et précisait qu'une partie « restreinte » de ce code ne serait pas publiée « car correspondant à des tests ou à des parties critiques pour la sécurité de l'infrastructure ».

« En revanche une documentation, publiée sur le GitLab [1], présentera les grands principes de sécurité mis en œuvre sur StopCovid (afin de respecter les demandes ou avis de la Cnil et les recommandations de l'Anssi). »

» L'éclairage de Pierrick Gaudry (CNRS)

Pierrick Gaudry, directeur de recherche CNRS travaillant au Loria (Laboratoire lorrain de recherche en informatique et ses applications sous tutelle du CNRS, d'Inria et de l'Université de Lorraine), répond à quelques questions de News Tank sur les enjeux liés à la publication du code source de StopCovid, le 27/05/2020.

Spécialiste de la cryptographie, il a notamment coécrit un article de vulgarisation intitulé *« Le traçage anonyme, dangereux oxymore »*, daté du 21/04/2020.

L'application StopCovid autorisée pour six mois maximum après la fin de l'état d'urge... *1/4*

Inria a indiqué qu'une partie « restreinte » du code ne serait pas publiée, « car correspondant à des tests ou à des parties critiques pour la sécurité de l'infrastructure ». Est-ce problématique selon vous ?

Cela ne me choque pas outre mesure que certaines parties ne soient pas ouvertes. Du côté des serveurs centraux, la sécurité va reposer sur de nombreux aspects qui ne sont pas facilement résumables au « code source » :

- Comment sont configurés les serveurs ?
- Comment sont gérés les accès à ces serveurs ?
- Comment sont gérés les back-up et la nécessaire redondance pour assurer que le système reste disponible 24/7 ?

Donc on est forcément obligé de mettre une limite quelque part à ce qu'on rend public. Par ailleurs, du côté du serveur, rien n'empêche l'État de faire tourner une variante avec des portes dérobées. Donc dévoiler l'intégralité du code source du serveur ne serait de toutes façons pas suffisant pour garantir qu'il ne fait rien de mal.

L'application StopCovid autorisée pour six mois maximum après la fin de l'état d'urge... *2/4*

Est-ce que les informations, les morceaux de code disponibles le 27/05, jour où le Parlement a débattu et s'est prononcé sur l'utilisation de StopCovid, sont suffisants pour étudier correctement les failles potentielles de cette application ?

De mon point de vue, il reste des points d'ombre critiques qui permettent difficilement de se prononcer, en particulier sur la mise en place des mixnets (composants techniques extrêmement importants pour se prémunir contre un serveur qui voudrait accumuler plus d'information que prévu par le protocole) et sur les liens avec la base Sidep [Système d'informations de dépistage].

Mesurer le rapport bénéfices/risques dans les conditions actuelles est impossible.

L'application StopCovid autorisée pour six mois maximum après la fin de l'état d'urge... ***3/4***

Concernant les aspects de la sécurité de cette application qui ne dépendent pas du code source, quelles garanties l'État pourrait-il apporter pour montrer « qu'il ne fait rien de mal » ? Est-il possible d'apporter une telle garantie dans ce cas ?

La réponse courte est : non, pour StopCovid c'est impossible. Après, selon la confiance que l'on accorde à certains services de l'État, on peut imaginer des audits et des surveillances qui apportent certaines garanties.

L'Anssi a certainement toutes les compétences pour cela. Par le passé, cette agence a déjà su montrer une certaine indépendance par rapport aux pressions des politiques. Mais sur ce projet, elle est partie prenante du développement, donc je suis plus perplexe.

L'application StopCovid autorisée pour six mois maximum après la fin de l'état d'urge... ***4/4***

D'autres Etats ont-ils choisi des solutions différentes pour garantir cette sécurité ?

Une solution, choisie par d'autres États européens, est de confier beaucoup moins de données au serveur central, en utilisant un protocole différent. Dans ce cas-là, le serveur ne détient que des informations que de toutes façons il est censé rendre publiques.

Cette approche est donc bien meilleure par rapport au risque de surveillance de masse. Mais tout n'est pas parfait non plus, car cela se fait au prix d'autres faiblesses ailleurs.

Le débat est d'ailleurs très vif dans la communauté au niveau international pour décider quelle approche est la meilleure, avec des considérations techniques et des considérations politiques qui souvent se marchent sur les pieds.

[1] Plateforme de DevOps (développement logiciel et administration des infrastructures informatiques) où Inria dépose le code source