

Délibération CNIL n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid »

24/04/2020

Dans le cadre de l'état d'urgence sanitaire lié au Covid-19 et notamment sur la stratégie de « déconfinement », la Commission nationale de l'informatique et des libertés (CNIL) a été saisie par Secrétaire d'Etat chargé du numérique, d'une demande d'avis relative aux conditions et modalités de l'éventuelle mise en œuvre de l'application « StopCovid » au regard de la réglementation française et européenne relative à la protection des données à caractère personnel. L'objectif de cette application, disponible sur smartphones et autres équipements mobiles, serait « d'informer les personnes l'ayant téléchargée du fait qu'elles ont été à proximité, dans un passé proche, de personnes diagnostiquées positives au COVID-19 et disposant de la même application, cette proximité induisant un risque de transmission du virus ».

Il est à noter qu'il s'agit d'une application de « suivi de contacts », et non de suivi des personnes exposées ou diagnostiquées positives au virus, qui reposerait notamment sur l'utilisation de la technologie de communication de proximité « Bluetooth » pour évaluer la proximité entre deux smartphones, sans recourir à une technologie de géolocalisation. Cette application repose sur la base du volontariat.

La Commission indique que cet avis vise à apporter, pour l'instant, « des éléments de réponse et à éclairer le Gouvernement sur l'analyse d'une telle application, étant précisé que le déploiement de cette application comme ses modalités exactes de mise en œuvre, sur les plans juridique, technique et pratique, ne sont pas encore arrêtés à ce stade ». La Commission devra donc être à nouveau saisie pour se prononcer sur les modalités définitives de mise en œuvre de ce dispositif.

La Commission estime que :

- S'agissant de l'existence de traitement de données de santé :

Le dispositif projeté est soumis aux règles de protection des données à caractère personnel, même si les protections prises apportent un haut degré de garantie pour minimiser le risque de ré-identification des personnes physiques associées aux données stockées, pour une durée nécessairement limitée, par le serveur central ;

Toute l'architecture du dispositif envisagée tend à ne faire remonter au serveur central que les pseudonymes générés par les applications associées aux personnes avec lesquelles un individu infecté a été en contact, et non le pseudonyme de ce dernier. La commission souligne que ce procédé minimise le risque de ré-identification de la personne infectée à l'origine d'une alerte, dans le plein respect des principes de protection des données personnelles.

Des garanties adaptées sont à prévoir, au titre desquelles l'atténuation des possibilités de ré-identification constitue une mesure essentielle.

- S'agissant de la notion de volontariat des utilisateurs de l'application :

Ce volontariat devrait être explicitement prévu dans les textes juridiques régissant ce dispositif comme dans l'information du public ;

La notion de volontariat doit donc impliquer que l'accès aux tests et aux soins ne saurait en aucun cas être conditionné à l'installation de l'application, que l'utilisation de cette application ne soit pas conditionnée ni à la possibilité de se déplacer, ni à l'accès de certains services (exemple : les transports en commun). Les utilisateurs de l'application ne devraient pas davantage être contraints de sortir en possession de leurs équipements mobiles. Enfin, les institutions publiques ou les employeurs ou toute autre personne ne devraient pas subordonner certains droits ou accès à l'utilisation de cette application.

- S'agissant de la base légale de l'application : la Commission recommande que le recours à un dispositif volontaire de suivi de contact pour gérer la crise sanitaire actuelle dispose d'un fondement juridique explicite et précis dans le droit national. Elle demande au gouvernement, le cas échéant et quel que soit le vecteur retenu, de la saisir à nouveau du projet de norme encadrant la mise en œuvre de l'application en cause lorsque la décision aura été prise et le projet précisé.

- S'agissant de l'admissibilité de l'atteinte à la vie privée par un dispositif de suivi de contacts : le gouvernement doit veiller à ce que l'atteinte portée à la vie privée demeure proportionnée à l'objectif poursuivi. Le respect du principe de proportionnalité se traduira notamment par une collecte et une conservation des données limitées à ce qui est strictement nécessaire, afin de minimiser l'atteinte portée à la vie privée des personnes.

- Enfin, concernant la configuration de l'application : le dispositif devrait être conçu de telle manière que le ministère chargé de la santé ou toute autre autorité sanitaire impliquée dans la gestion de la crise sanitaire puisse assurer la responsabilité de traitement. De plus, une analyse d'impact sur la protection des données devra être réalisée avant toute mise en œuvre d'un tel dispositif. La Commission détaille dans sa délibération les points qu'elle estime essentiels concernant la sécurité des données personnelles (clés de chiffrement, algorithmes cryptographiques...).