Projet de mise en place de l'application Stop-Covid.

Sans qu'il soit question pour moi, de vous exprimer mon avis personnel sur cette application, je vous expose ci-dessous, l'avis de la CNIL sur cette application :
L'application Stop Covid peut "potentiellement" participer à la lutte contre le Covid-19, mais "n'en possède pas moins des limites, tant intrinsèques que liées à son insertion dans une politique sanitaire globale".
C'est ce qu'estime la **Cnil** dans sa délibération publiée dimanche 26 avril 2020. L'instance, qui met en garde contre tout "solutionnisme technologique", insiste sur le fait que le dispositif "pose des questions inédites en termes de protection de la vie privée". Elle détaille les limites que présente la solution, appelant notamment à garantir la sécurité des données traitées.
Dans sa délibération adoptée vendredi 24 avril 2020 et rendue publique dimanche, la Cnil fait part de son assentiment quant au projet d'application gouvernemental Stop Covid, estimant toutefois que l'atteinte qu'elle est susceptible de porter à la vie privée ne sera admissible que si "le gouvernement peut s'appuyer sur des éléments suffisants pour avoir l'assurance raisonnable qu'un tel dispositif sera utile à la gestion de la crise, et notamment à la sortie du confinement de la population". Elle appelle "à la plus grande prudence" de l'exécutif sur la collecte de données personnelles.
La commission, qui avait été saisie par le secrétaire d'État chargé du Numérique, Cédric O, le 20 avril 2020, demande en outre à être de nouveau saisie après le débat au Parlement prévu cette semaine, afin de se "prononcer sur les modalités définitives de mise en oeuvre du dispositif".
Pour rappel, le projet gouvernemental de "suivi de contacts" consiste à pouvoir informer un utilisateur de l'application que son téléphone s'est trouvé à proximité, au cours des jours précédents, de celui d'une personne ayant ultérieurement été diagnostiquée positive au Covid-19, par la collecte de traces pseudonymes.
Pour l'autorité administrative indépendante, **la collecte et la conservation des données devront se limiter "à ce qui est strictement nécessaire"** et devront revêtir **un caractère temporaire**. Toutes les données devront être supprimées dès lors que l'utilité de l'application "ne sera plus avérée". Elle met **en lumière plusieurs limites de l'application** : seuil de la population devant installer la solution pour garantir son efficacité, vulnérabilité des personnes ne disposant pas d'équipement mobile adéquat, porteurs sains qui utiliseraient l'application sans déclencher d'alerte…
L'application doit par ailleurs être déployée "**dans le cadre d'une réponse sanitaire globale**", pointe l'instance. Alertant contre la "tentation du solutionnisme technologique", la Cnil appelle le gouvernement à identifier les autres solutions à mettre en oeuvre en parallèle : mobilisation des personnels de santé, disponibilité des masques et des tests, organisationdes dépistages, isolement des personnes infectées, etc. "Ce déploiement doit s'inscrire dans un plan d'ensemble." Elle recommande également de mettre en place un suivi documenté de l'impact du dispositif, afin de permettre aux pouvoirs publics de "décider de manière éclairée son maintien ou non".
La Cnil insiste également sur la sécurité des données personnelles, "garantie indispensable, eu égard à la sensibilité" du dispositif. Elle conseille la mise en oeuvre de "mesures de sécurité organisationnelles et techniques de très haut niveau" concernant le serveur chargé de la centralisation des identifiants des personnes exposées, attirant notamment l'attentionsur "les

clés de chiffrement permettant l'accès aux identifiants des personnes concernées", qui pourraient "être protégées via des modules de sécurité matériels".
"Seuls des algorithmes cryptographiques à l'état de l'art doivent être mis en oeuvre, afin d'assurer l'intégrité et la confidentialité des échanges", note la commission. L'algorithme 3DES, envisagé à ce stade, "ne devrait en principe plus être utilisé", selon les recommandations de l'Anssi, pointe-t-elle. Elle estime en **outre nécessaire que des mesures soient mises en oeuvre pour éviter de pouvoir recréer un lien entre pseudonymes temporaires délivrés par l'application et informations spécifiques au téléphone liées au Bluetooth permettant d'identifier les utilisateurs .**
Par ailleurs, observant que **le projet ne prévoit pas de d'enrôlement des personnes lors de la première utilisation de l'application", la Cnil note qu'il pourrait en résulter "un risque d'attaque accru".** Plus largement, elle souligne l'importance de rendre public le code source de l'application, du serveur central et leur paramétrage, et de garantir le libre accès aux protocoles utilisés. "Il s'agit tant de permettre à la communauté scientifique de contribuer à l'amélioration constante du dispositif et à la correction des éventuelles vulnérabilités que de garantir une parfaite transparence vis-à-vis de l'ensemble des citoyens."
Prenant acte du fait que l'installation et l'utilisation de l'application reposent sur une démarche volontaire, l'instance estime que cet élément est "déterminant pour assurer la confiance dans le dispositif et favoriser son adoption par une partie significative de la population". Elle appelle cependant à ce que ce volontariat ne se traduise pas uniquement par le choix, pour l'utilisateur, "de télécharger puis de mettre en oeuvre l'application […] ou la faculté de la désinstaller".
"**Le volontariat signifie aussi qu'aucune conséquence négative n'est attachée à l'absence de téléchargement ou d'utilisation de l'application. Ainsi, l'accès aux tests et aux soins ne saurait en aucun cas être conditionné à l'installation de l'application", insiste la commission. Pour elle, l'utilisation de cette application ne devrait pas non plus conditionner la possibilité de se déplacer librement lors de la levée du confinement, d'utiliser les transports en commun ou d'accéder à certaines zones, entreprises ou institutions publiques, ce qui constituerait une "discrimination".**
En outre, **les utilisateurs de l'application "ne devraient pas davantage être contraints de sortir en possession de leurs équipements mobiles".** "**À ces conditions l'utilisation de Stop Covid pourra être regardée comme réellement volontaire.** Des choix différents […] porteraient une atteinte bien plus considérable au droit à la protection des données à caractère personnel et au respect de la vie privée." Par ailleurs, l'application "n'a pas pour objet de surveiller le respect des mesures de confinement", ni de réaliser un suivi du nombre de personnes infectées, note la Cnil.
La présence de données à caractère personnel **impose de "prévoir des garanties adaptées d'autant plus fortes que les technologies sont intrusives, garanties au titre desquelles l'atténuation des possibilités de ré-identification constitue une mesure essentielle**", note également l'autorité administrative. Selon elle, une ré-identification des personnes avec lesquelles l'utilisateur a été en contact à partir de leurs pseudonymes est possible.
Cependant, elle relève que la solution comporte des garanties qui viennent minimiser ce risque. Ainsi, elle souligne notamment que l'architecture choisie tend à éviter "que soit centralisée dans un serveur une liste des personnes qui se déclarent malades", et fait remonter au serveur central uniquement les pseudonymes générés par les applications associées aux personnes avec lesquelles un individu infecté a été en contact.