

Application norvégienne de traçage des infections à la Covid-19 : un très mauvais exemple

Valentin Conrad, le 15 octobre 2020

Nous mettons en ligne, de manière périodique, les contributions d'auteurs externes nous ayant fait l'honneur d'accepter d'accompagner le lancement de Swissprivacy. Nous accueillons cette semaine la contribution de Valentin Conrad, juriste senior auprès de l'École polytechnique fédérale de Lausanne

Le 12 juin dernier, l'autorité de protection des données norvégienne (l'APD) interdisait temporairement le traitement des données personnelles opéré par l'Institut norvégien de santé publique (ci-après : « l'Institut »), lequel avait lancé une application mobile de traçage pour lutter contre la Covid-19, dénommée « Smittestopp » (décision disponible sur le [site de l'Institut](#), mais un résumé en anglais peut être consulté [ici](#)). Environ 14% de la population norvégienne de plus de 16 ans l'avaient téléchargée.

Contrairement à d'autres applications de traçage, l'application norvégienne entendait utiliser la géolocalisation (par localisation GPS), en plus d'un système de traçage de proximité par Bluetooth. De plus, les données suivantes étaient notamment enregistrées dans un cloud centralisé pendant 30 jours au maximum (mais réduit à 10 jours maximum par la suite) : numéro de téléphone portable, âge, position GPS en continu, identifiant unique qui suit le numéro de téléphone, opérateur mobile, enregistrement des contacts Bluetooth. Au demeurant, la solution imaginée s'écarterait des autres modèles adoptés par d'autres pays, en ce sens que l'application servait deux buts distincts : (i) détecter les personnes potentiellement infectées et ralentir la propagation du virus, et (ii) analyser les données à des fins de recherche pour contrôler les effets de mesures prises par l'Institut.

Dans sa décision, l'APD notait d'emblée que la surveillance étatique des mouvements des individus et de leurs contacts impliquait une très grande interférence avec leur vie privée. Or, même dans une situation exceptionnelle, telle que la pandémie de Covid-19, les droits fondamentaux devaient être respectés. L'autorité relevait ainsi que plus l'intrusion dans la vie privée est grande, plus la nécessité du traitement des données personnelles doit être soumise à des exigences strictes. Par conséquent, le traitement des données personnelles devait être strictement nécessaire pour atteindre l'objectif affiché de santé publique. Par ailleurs, l'APD rappelait certains principes fondamentaux de protection des données à l'instar

de la limitation du but du traitement à des fins spécifiques et sans équivoque, la minimisation des données (qui suppose que les données récoltées soient adéquates, pertinentes et limitées à ce qui est nécessaire aux fins pour lesquelles elles sont traitées), ou encore la transparence par rapport aux traitements de données envisagés. Elle se référait, de surcroît, aux Lignes directrices du Comité Européen de la Protection des données relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de Covid-19 et aux Considérations éthiques pour guider les utilisations de technologies de traçage en lien avec la Covid-19, publiées par l'Organisation mondiale de la santé le 28 mai 2020.

Outre des éléments techniques gérés de façon plutôt aléatoire (notamment pour sécuriser les données personnelles), l'APD constatait les problèmes suivants :

- puisque l'application servait deux buts distincts, le risque que les utilisateurs potentiels ne téléchargeassent pas l'application était plus grand, car les utilisateurs pourraient être gênés de télécharger une application combinant plusieurs objectifs. Par ailleurs, pour être utile, l'application n'avait pas besoin du même seuil minimal d'utilisateurs : si 10% de la population suffiraient à des fins de recherche, 60% au moins de la population devraient utiliser l'application pour ralentir la propagation du virus. Une séparation des finalités de traitement s'avérerait donc nécessaire ;
- la centralisation du stockage des données s'exposait à un risque accru de violation des droits des personnes concernées. Une décentralisation du stockage des données serait donc recommandée ;
- pour être proportionnée, l'application de traçage aurait dû apporter des avantages sociaux. Or, au moment de la prise de décision, seulement 0,01% de la population norvégienne avait été infectée par le virus et le risque d'infection avait considérablement diminué. De plus, les mesures de contrôle des infections (tests, isolement, détection manuelle des infections, etc.) semblaient bien fonctionner, et l'infection Covid-19 était considérée comme étant suffisamment contrôlée. Enfin, en raison du faible nombre de personnes notifiées, l'utilité de l'application n'avait pas pu être démontrée ;
- les informations personnelles collectées via l'application ne se limitaient pas à ce qui était nécessaire pour atteindre les objectifs, contredisant ainsi le principe de minimisation des données. En particulier, l'Institut n'avait pas su démontrer en quoi il serait nécessaire de collecter des données GPS ;
- la garantie du droit d'accès aux données personnelles n'était pas assurée.

En définitive, cette décision est importante puisqu'elle est une des seules à avoir interdit -

à tout le moins temporairement – l'utilisation d'une application de traçage. Il faut dire que les choix opérés par l'Institut n'étaient guère judicieux (centralisation des données ; pluralité de finalités ; collecte de données GPS ; etc.). Par ailleurs, l'APD a mis en exergue un principe cardinal en protection des données, celui de la proportionnalité. Il est du reste regrettable que certaines autorités de protection des données n'aient pas eu l'indépendance nécessaire (ni le courage ?) pour commenter de façon plus nuancée et critique le respect de ce principe par leurs offices de santé publique respectifs en lien avec le lancement de leur application national de traçage.

Proposition de citation : Valentin CONRAD, Application norvégienne de traçage des infections à la Covid-19 : un très mauvais exemple, 15 octobre 2020 *in* www.swissprivacy.law/16

 Les articles de [swissprivacy.law](http://www.swissprivacy.law) sont publiés sous licence creative commons CC BY 4.0.