_swissprivacy.law

SocialPass : les recommandations du PFPDT confirment de graves lacunes

Sylvain Métille, le 27 août 2021

Au terme d'une procédure d'établissement des faits longue et difficile, le PFPDT a adressé aux exploitants privés de l'application SocialPass plusieurs recommandations visant notamment à améliorer la sécurité technique de l'application et à limiter de manière proportionnée l'accès des autorités sanitaires cantonales aux données enregistrées de manière centralisée. Comme il ressort du rapport final publié aujourd'hui, les exploitants ont finalement accepté de mettre en œuvre les principales recommandations du PFPDT, après les avoir initialement contestées.

Nota bene (Livio di Tria) : Cette publication a été initialement publiée sur le blog personnel du Prof. Sylvain Métille. Ce dernier nous a cependant fait le plaisir de nous autoriser à la republier au sein de swissprivacy.law. Désormais connue comme l'affaire SocialPass, nous avions déjà eu l'occasion en juin dernier de nous pencher dessus, sur la base d'un communiqué de presse du PFPDT (swissprivacy.law/78/). Pour sa part, la contribution du Prof. Sylvain Métille dissèque la récente recommandation du PFPDT. Merci à lui !

Le but n'est pas de s'acharner sur l'application SocialPass, mais pour une fois que PFPDT publie des recommandations en matière de protection des données, il est nécessaire de les examiner en détail. Elles devraient aussi permettre d'amener un peu de clarté dans un processus qui est resté opaque depuis de nombreux mois, même s'il est imposé à de nombreux clients de restaurants.

Je me concentrerai principalement sur les questions juridiques, même si le rapport mentionne un certain nombre de risques techniques, des lacunes d'organisation et des difficultés importantes pour le PFPDT à obtenir des réponses à ses demandes.

En bref

Le PFPDT a identifié de nombreuses lacunes et émis dix recommandations (acceptées en partie seulement par les sociétés concernées). Le PFPDT peut maintenant porter l'affaire devant le Tribunal administratif fédéral pour rendre ses recommandations contraignantes.

L'établissement des faits a d'abord révélé des déficiences organisationnelles et techniques. Il a ensuite confirmé que les exploitants du SocialPass ont accordé aux autorités sanitaires des cantons de Vaud et du Valais un accès direct à la banque de données centrale, leur permettant ainsi d'effectuer des recherches ciblées à discrétion, ce qui contrevient au principe de proportionnalité. D'autres recommandations concernent l'exhaustivité des informations fournies aux utilisateurs, l'exportation de numéros de téléphone vers les USA en vue de leur vérification et la configuration de la plateforme Microsoft Azure sur laquelle se trouve la banque de données centralisée.

Pourquoi des recommandations ?

Dès juillet 2020, le PFPDT a reçu des demandes de citoyens et de médias. Il a pris contact avec les responsables de SocialPass (SwissHelios Sàrl et NewCom4U Sàrl) en novembre 2020 et ouvert formellement une procédure d'établissement des faits (art. 29 LPD) en décembre 2020. Au terme d'une procédure longue et difficile, il a rendu le 4 août 2021 un rapport final et des recommandations, rendues publiques le 20 août 2021.

Qui est l'autorité compétente ?

Le PFPDT a considéré qu'il était compétent s'agissant d'entreprises privées. Ce raisonnement peut être suivi. Dans ce cas, on peut s'étonner de la participation d'autorités cantonales à deux vidéoconférences mentionnées sans plus de détails dans le rapport, même si la collaboration entre autorités n'est pas rare.

En revanche, il y a un conflit d'intérêts évident lorsque la même personne intervient simultanément en qualité d'avocats des deux sociétés visées par la procédure et de préposé cantonal à la protection des données. Le PFPDT n'a pourtant pas fait de commentaires particuliers à ce sujet.

Qui est le responsable du traitement ?

Les deux sociétés sont des responsables du traitement conjoint, mais il n'a pas été possible de déterminer la répartition de leurs responsabilités. Cette analyse est cohérente avec la base de données centralisée sans séparation des établissements ou cantons. Elle l'est moins avec l'esprit de l'Ordonnance COVID-19 situation particulière.

Les indications dans les différents documents sont contradictoires dans la mesure où certains mentionnent l'un, l'autre ou les deux sociétés en tant que responsables du traitement. Le

PFPDT a retenu une violation du principe de transparence. En effet, les personnes concernées ne sont pas en mesure de déterminer avec certitude quelle personne morale traite leurs données et à qui, le cas échéant, elles devraient adresser une demande d'accès.

Une base de données centralisée est-elle admissible ?

Le PFPDT considère que sur le principe, une base de données centralisée n'est pas exclue si des mesures de sécurité adéquates sont prises. Je peux aussi admettre que le traitement est confié à un (vrai) tiers, mais je ne pense en revanche pas que l'on puisse considérer les deux sociétés comme des sous-traitantes au sens de l'art. 10a LPD comme semble le mentionner à un moment le PFPDT.

En revanche, le droit fédéral ne prévoit pas d'accès direct par les médecins cantonaux, ni de fonction de recherche par nom par exemple (ce qui conduirait à la création de profils de personnalités).

Le principe est au contraire que le médecin cantonal peut seulement demander la liste des personnes présentes dans un établissement déterminé à un moment donné. L'établissement peut ainsi jouer un rôle de contrôle et éviter les abus.

Le droit cantonal peut-il prévoir une traçabilité étendue ou des accès directs ?

Non. À raison, le PFPDT retient que les documents évoqués dans les cantons de Vaud et Valais ne constituent pas des normes suffisantes pour justifier un accès direct. La directive vaudoise a d'ailleurs été abrogée depuis.De plus, un tel accès direct n'a pas été retenu dans la législation fédérale et ne répond pas à un intérêt public.On notera au passage que la base de données centralisée en mains du canton et l'accès direct sont la solution qui a été retenue par le canton de Berne.

Les données pouvaient-elles être communiquées aux USA ?

Le PFPDT retient que les personnes concernées n'étaient pas informées de la communication des numéros de téléphone à Twilio aux USA. Le rôle (et les conditions) du prestataire américain ne sont pas claires et les responsables de SocialPass n'avaient aucune garantie suffisante de la part du prestataire établi dans un État dont le niveau de protection des données n'est pas adéquat.

La sécurité des données est-elle assurée ?

Pas vraiment. Le PFPDT a émis plusieurs recommandations, notamment pour éviter la conservation illimitée des numéros de téléphones mobiles, améliorer la configuration de la plateforme Microsoft Azure, éliminer les vulnérabilités identifiées, mettre en place une authentification forte pour limiter les risques d'accès indus et renoncer aux traitements d'identifiants inutiles comme le numéro IMEI ou l'UID provenant de Google Firebase. Finalement, le PFPDT a encore constaté l'absence de toute documentation relative à la sécurité des données.

Quelques questions restantes

J'avais personnellement exercé mon droit d'accès en juin et les deux sociétés m'avaient indiqué être des sous-traitants du médecin cantonal vaudois (et pas des responsables du traitement, ce qui contredit fondamentalement les constatations du PFPDT).

Plus inquiétant, le médecin cantonal vaudois m'avait confirmé qu'il était bien le responsable du traitement. À ce moment, la directive vaudoise qui prévoyait un accès direct (mais contestée par le PFPDT) avait de plus déjà été abrogée.

Les collaborateurs d'un canton n'avaient pas accès aux données des résidents d'un autre canton. Si cela semble a priori une bonne nouvelle, c'est assez troublant à y regarder de plus près. Dans des situations limitées, une autorité cantonale peut demander les données des personnes présentes dans un établissement public de son canton. C'est le lieu de l'établissement qui est relevant et pas le canton d'origine des clients. La collecte des données dans un établissement devait permettre d'identifier les personnes présentes dans cet établissement, pas de rechercher les établissements fréquentés (potentiellement aussi hors canton) par un citoyen du canton qui effectue la recherche.

Et avec la nouvelle LPD ?

Si la nouvelle LPD était déjà en vigueur, le PFPDT aurait pu rendre une décision et imposer des modifications. Il aurait aussi pu assortir ses demandes de menace de sanctions pénales, ce qui lui aurait vraisemblablement permis d'avoir les informations qu'il n'a pas pu obtenir aujourd'hui.

Finalement, il est probable que les dirigeants des deux sociétés auraient été condamnés pénalement à une amende pouvant aller jusqu'à CHF 250'000.- pour violation du devoir d'information, mesures de sécurité insuffisantes et transfert de données à l'étranger sans garanties suffisantes.

_swissprivacy.law

Proposition de citation : Sylvain MÉTILLE, SocialPass : les recommandations du PFPDT confirment de graves lacunes, 27 août 2021 *in* www.swissprivacy.law/87