Failles dès la conception dans l'affaire mesvaccins.ch

Alexandre Barbey, le 15 octobre 2021

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) a émis trois recommandations à l'issue d'une procédure d'établissement des faits à l'encontre de la fondation mesvaccins dans son rapport final publié le 7 septembre 2021. Des failles dans les mesures techniques et organisationnelles sont mises en cause.

« Le carnet de vaccination électronique suisse : sûr – pratique – durable »[1]. Ce slogan provient d'un dépliant de 2018 créé à l'attention des médecins, vantant les avantages de la plateforme en ligne gérée par la fondation mesvaccins. Or, depuis, beaucoup d'encre a coulé sur ce scandale concernant d'affolantes failles de sécurité (art. 5 let. h nLPD) au point que la plateforme a été fermée temporairement dans le courant du mois de mars 2021, puis définitivement en mai. Entretemps, la fondation a finalement annoncé le 24 août 2021 sa prochaine liquidation. Le rapport final de la procédure d'établissement des faits (art. 29 al. 1 LPD), ouverte le 22 mars 2021, a été publié par le PFPDT le 7 septembre dernier. Trois recommandations au sens de l'art. 29 al. 3 LPD ont été émises.

En qualifiant l'affaire mesvaccins comme étant une erreur de système au sens de l'art. 29 al. 1 let. a LPD, le Préposé fédéral a consacré une partie non négligeable de son rapport aux mesures techniques et organisationnelles que la fondation mesvaccins aurait dû mettre en place afin d'éviter les failles de sécurité existantes. En effet, il s'est avéré que ces dernières étaient telles que les données contenues sur la plateforme en ligne mesvaccins.ch ont pu être consultées, modifiées ou supprimées par des tiers non autorisés. L'un des problèmes relevait du fait que les mécanismes mis en place permettant de vérifier si aucun accès indu n'avait eu lieu étaient obsolètes et cela à double titre. Il faut rappeler à cet égard qu'avant le scandale, il était prévu que la fondation mesvaccins soit chargée d'établir un module ayant la même fonction que l'actuel certificat Covid. Or bien que ce module dont le développement est plus récent que la plateforme originelle mesvaccins.ch, celui-là ne respectait pas davantage les exigences de sécurité de protection des données.

Le Préposé fédéral a insisté sur l'importance d'un processus efficace de journalisation des accès. Celui utilisé par la plateforme était déficient pour plusieurs raisons : les données journal n'étaient conservées que 30 jours, n'étaient pas protégées contre une quelconque manipulation et un système d'alerte automatique aurait dû être mis en place afin que les gérants de la plateforme soient avertis en cas de comportement frauduleux. Pour cette raison,

personne ne peut déterminer si, d'une part, des accès sans autorisation à la plateforme ont eu lieu, et, d'autre part, quelles données auraient pu être modifiées ou supprimées sans droit. Un rapport établi par une entreprise experte en cybersécurité, mentionné par le PFPDT, indique qu'il aurait suffi à un pirate d'accéder au compte d'un seul professionnel de la santé inscrit sur la plateforme pour avoir accès aux données de toutes les personnes qui l'ont utilisée. Ce rapport indique également que ces problèmes existaient au moins quelques mois avant la révélation au public des failles de la plateforme par le magazine Republik.ch.

Au vu de ces problèmes liés à l'intégrité des données, le Préposé fédéral a recommandé que le principe d'exactitude soit respecté, ce qui implique que les données traitées par la fondation doivent être correctes. Les éléments exposés nous font penser qu'il sera difficile de s'en assurer.

Ces éléments nous permettent de signaler que, bien que l'obligation de la protection des données dès la conception, à charge du responsable du traitement, ne soit pas encore connue du droit suisse, elle a néanmoins déjà toute son importance. De plus, le rapport indique, malgré le fait que les données stockées sur la plateforme soient actuellement inaccessibles en raison de la liquidation de la fondation, qu'elles doivent néanmoins l'être d'une manière qui soit conforme aux principes de finalité et de sécurité de la protection des données. Autrement dit, il ne faudrait pas, alors même que la plateforme a été fermée, que des accès indus soient encore possibles. L'obligation de *privacy by design*, permet en effet, de par sa logique *ex ante*, d'éviter un bon nombre de risques liés à la protection des données avant leur réalisation.

D'autres questions juridiques se sont posées dans cette affaire. Tout d'abord, il existe, en rapport avec la liquidation de la fondation, le problème de ce qu'il adviendra des données de vaccination stockées sur la plateforme. En effet, un nombre non négligeable de personnes n'y ont plus accès, ce qui est notamment particulièrement problématique dans le cas où ces personnes n'ont plus de version papier de leur carnet de vaccination, ou une quelconque autre manière de savoir quels vaccins leur ont été inoculés. Le Préposé fédéral a ainsi recommandé qu'une information active à ce sujet soit donnée aux personnes concernées. On peut constater que la fondation communique régulièrement au public sur les bribes de son site web. Une solution a été trouvée pour les personnes qui ont utilisé l'application myViavac sur leur téléphone, qui reprenait les données de la plateforme mesvaccins.ch, leur permettant de récupérer leurs données vaccinales. Quant aux personnes qui n'utilisaient que la plateforme mesvaccin.ch, aucune solution n'a encore été proposée, bien que la fondation affirme que des discussions avec les autorités afin d'en trouver sont menées. La récente entrée en

vigueur de l'art. 242b LP permet de faciliter les démarches dans le contexte de la liquidation de la fondation.

Ensuite, le Préposé fédéral a discuté des frais encourus par les personnes concernées ayant exercé leur droit d'accès afin d'établir des copies certifiées de leur pièce d'identité, celles-ci étant requises par la fondation. Il insiste à cet égard sur le caractère exceptionnel de la participation aux frais de la personne concernée lors d'une procédure de droit d'accès, hypothèse prévue par l'art. 2 OLPD. L'exception se veut restrictive et les difficultés actuelles de la fondation ne sauraient remplir l'hypothèse de l'art. 2 al. 1 let. b OLPD, permettant de demander à la personne concernée de participer aux frais, à savoir un volume de travail considérable. Le Préposé a donc indiqué dans sa recommandation que les frais encourus par les personnes concernées afin d'établir des copies certifiées de leurs documents d'identité devront être remboursés par la fondation. De plus, les personnes concernées devront être informées de l'éventuelle atteinte à l'exactitude des données.

Les recommandations émises par le Préposé fédéral ont été acceptées par la fondation. Le problème majeur de l'affaire reste donc celui pour les personnes concernées de pouvoir récupérer leurs données. Dans l'ensemble, cette affaire nous montre qu'une logique *ex post* telle que celle utilisée par la fondation mesvaccins n'a actuellement plus sa place. Les outils qu'amènera la révision de la LPD, tels que l'analyse d'impact relative à la protection des données (art. 22 nLPD), l'obligation de *privacy by design* (art. 7 al. 1 et 2 nLPD) ainsi que l'annonce des violations de sécurité des données (art. 24 al. 1 nLPD) permettront, nous en sommes convaincus, d'éviter d'avoir à déplorer de nouveaux scandales du même genre.

Proposition de citation : Alexandre Barbey, Failles dès la conception dans l'affaire mesvaccins .ch, 15 octobre 2021 *in* www.swissprivacy.law/94