Date de dépôt :23 juin 2021

Réponse du Conseil d'Etat

à la question écrite urgente de M. Christo Ivanov : Quand les données privées deviennent publiques

Mesdames et
Messieurs les députés,

En date du 21 mai 2021, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

A l'ère de la numérisation de la société avec une connexion permanente à l'internet, un nombre de données personnelles toujours plus important circulent. Des cybercriminels sont susceptibles d'obtenir ces données personnelles en utilisant des ruses parfois grossières (comme le faux support technique) ou en déployant leur savoir-faire informatique à mauvais escient. Parmi nos données personnelles, les données médicales figurent peut-être parmi les données les plus sensibles.

La société M3 propose à la population genevoise une plateforme informatique permettant de s'inscrire en vue d'un dépistage covid. Il suffit d'enregistrer son numéro d'assuré et l'informatique fait le reste. Identité, date de naissance, numéro AVS, adresse, tout apparaît automatiquement. Malheureusement, le système présente une grave faille de sécurité qu'un pirate informatique pourrait mettre à profit pour obtenir les données personnelles de tous les assurés du pays. Le nombre d'entrées n'est pas limité, de sorte qu'on peut saisir autant de fois qu'on veut jusqu'à tomber sur un numéro correspondant à un assuré et obtenir ses données personnelles. Une telle légèreté laisse pantois, d'autant plus que M3 était consciente du risque. La société a délibérément choisi de ne pas prendre les mesures empêchant les saisies répétées, préférant limiter le nombre de demandes dans un temps donné.

Le Conseil d'Etat porte une lourde responsabilité par rapport à cette potentielle fuite de données, ayant mandaté M3 sans prendre l'élémentaire précaution de vérifier le niveau de sécurité proposé par l'entreprise.

Mes questions sont les suivantes :

1) ***Quelles ont été les exigences en matière de sécurité envers M3 ?***
2) ***L'intervention de la Confédération ne constitue-t-elle pas un vilain taquet derrière les oreilles pour le gouvernement qui ne remplit pas ses obligations au niveau cantonal mais aussi fédéral ?***
3) ***Est-il prévu de maintenir l'accès de M3 aux données personnelles des citoyens résidant en Suisse vu la légèreté dont elle fait preuve ?***
4) ***A-t-on évalué le risque que les données auxquelles M3 a accès puissent faire l'objet d'un mauvais usage ?***

RÉPONSE DU CONSEIL D'ÉTAT

1) Quelles ont été les exigences en matière de sécurité envers M3 ?

A l'automne 2020 – au plus fort de la deuxième vague –, m3 Sanitrade a proposé des solutions concrètes de testing à très haut débit pour renforcer le dispositif cantonal de tests à un moment crucial. Alors que l'entreprise, en un temps très court, parvenait à proposer des solutions concrètes et à répondre à tous les critères d'exigence des autorités sanitaires – plan de protection, infrastructures, accueil des patients, réalisation des tests et leur interprétation, information aux patients, sécurité – elle a reçu l'accord de l'Etat pour exploiter un grand centre de test. Les exigences de sécurité informatique à son endroit étaient et restent les mêmes que celles qui prévalent pour les acteurs maniant des données personnelles sensibles, notamment au sein des institutions de santé.

L'entreprise m3 Sanitrade a toujours montré à la direction générale de la santé qu'elle prenait très au sérieux la protection des données personnelles et mettait en place tous les moyens techniques et organisationnels nécessaires afin de protéger ces données contre l'accès non autorisé, la perte, l'utilisation abusive ou la falsification. Le système de requête informatique qui permet de remonter des données administratives à partir du numéro d'assurance-maladie est le même que celui qu'utilisent les cabinets médicaux, institutions de santé et autres acteurs de la santé du canton. Il convient de relever en outre qu'aucune donnée médicale ou résultat d'analyse ne transite, à aucun moment, par les serveurs de m3 Sanitrade.

2) L'intervention de la Confédération ne constitue-t-elle pas un vilain taquet derrière les oreilles pour le gouvernement qui ne remplit pas ses obligations au niveau cantonal mais aussi fédéral ?

Non, elle illustre simplement l'attention qui est portée, dans ce pays, à la protection des données personnelles. Aucune faille critique n'a été relevée et les informations données dans la presse se sont avérées erronées (cf. infra), notamment sur le fait qu'aucune limite n'était opposée au nombre d'entrées possibles. Ce point est repris dans la présente question écrite urgente et il est inexact : le système limitait dès l'origine les entrées multiples.

3) Est-il prévu de maintenir l'accès de M3 aux données personnelles des citoyens résidant en Suisse vu la légèreté dont elle fait preuve ?

Affirmer que m3 Sanitrade aurait eu une gestion légère, non professionnelle ou non éthique des données dont elle avait besoin pour offrir des solutions de testing, à très court terme, à la population genevoise est erroné et injustifié. Il n'est tout simplement pas possible de remplir une telle mission sans ces données. L'entreprise citée traite ces données selon les mêmes critères de sécurité que les médecins genevois et les cliniques privées. Les centres de tests de m3 Sanitrade fournissent une capacité de test essentielle au canton pour lutter contre l'épidémie de COVID-19. Il faut rappeler que ces capacités ont précisément fait défaut tant durant la première vague qu'au début de la deuxième.

4) A-t-on évalué le risque que les données auxquelles M3 a accès puissent faire l'objet d'un mauvais usage ?

L'architecture de l'interface utilisateur du site www.m3-test.ch a été établie de façon à raccourcir les temps d'admission et à limiter les files d'attente, à éviter les erreurs de saisie et à simplifier l'expérience des utilisatrices et utilisateurs, tout en maintenant les standards de sécurité informatique en vigueur.

Les limitations déjà en place avant la publication de l'article du *Matin Dimanche* le 16 mai 2021 rendaient la probabilité de récupération des données d'une assurée ou d'un assuré extrêmement faible, de même que le risque de collision (découverte par hasard d'un numéro de carte d'assurée ou d'assuré).

Après avoir étudié les historiques d'utilisation de cette fonctionnalité, le service informatique de m3 Sanitrade n'a constaté aucun usage anormal susceptible de dénoter une tentative de récupération de données personnelles. En l'état, aucune preuve d'attaque malveillante destinée à la récupération de

données personnelles n'a été trouvée, et il est extrêmement improbable qu'une fuite d'information, qu'un accès indu ou qu'un traitement illicite ait eu lieu.

La société m3 Sanitrade a décidé d'abaisser encore le nombre de tentatives maximales par utilisatrice ou utilisateur à 10. Afin de rendre visible cette limite du nombre de requêtes, le message renvoyé lorsque l'utilisatrice ou l'utilisateur entre de façon erronée son numéro d'assurée ou d'assuré de trop nombreuses fois sera modifié. Elle ou il recevra un message explicite indiquant que le nombre d'essais est atteint et qu'elle ou il doit essayer à nouveau plus tard.

Ainsi, le risque de mauvais usage par un tiers est très faible et ne constitue aucunement un obstacle à la poursuite du mandat de m3 Sanitrade, dont nous savons que la capacité de tests est essentielle en cette période de voyages et de vacances à venir.

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Michèle RIGHETTI	Serge DAL BUSCO