



Intervention parlementaire

Réponse du Conseil-exécutif

N° de l'intervention : 093-2021
Type d'intervention : Interpellation
Motion ayant valeur de directive : ☐
N° d'affaire : 2021.RRGR.162

Déposée le : 05.06.2021

Motion de groupe : Non
Motion de commission : Non
Déposée par : Fuhrer-Wyss (Burgistein, PS) (porte-parole)
Binggeli (Biel/Bienne, PS)
Cosignataires : 0

Urgence demandée : Oui
Urgence accordée : Oui 10.06.2021

N° d'ACE : 912/2021 du 18 août 2021
Direction : Direction de la santé, des affaires sociales et de l'intégration
Classification : -

Garantir la protection des données lors de l'enregistrement des données des personnes qui vont dans les établissements de restauration

La pandémie de coronavirus nous a confronté·e·s à un grand nombre de défis nouveaux. De nombreuses mesures encore inimaginables il y a quelques mois se sont avérées nécessaires et utiles. D'autres ont été prises pour accompagner les étapes de réouverture tant attendues. Une chose est évidente : le traçage précis des contacts pendant la pandémie est, pour des raisons de santé, important et opportun. Cependant, l'enregistrement centralisé des données que le canton de Berne a l'intention d'instaurer dans le cadre de l'ouverture des établissements de restauration est on ne peut plus problématique pour des raisons de protection des données. Selon des informations rendues publiques, la banque de données « Swiss Contact Tracing Database », actuellement utilisée dans de nombreux établissements de restauration, est un vrai cauchemar du point de vue de la protection des données. En effet, les données des personnes concernées provenant d'applications d'enregistrement numériques suisses leaders seraient mises en convergence et analysables de diverses manières ; un historique des visites deviendrait possible. Il faut garantir la protection des données.

Le Conseil-exécutif est chargé de répondre aux questions suivantes :

1. Comment la protection des données est-elle garantie ?
2. Pourquoi n'existe-t-il pas sur le plan technique des barrières de sécurité empêchant l'obtention de données personnelles ?
3. Quelles barrières techniques existe-t-il permettant l'anonymisation des données ?
4. La fédération Gastro Suisse propose 16 applis différentes sur son site Internet ; aucune d'entre elles n'a été soumise à des tests de sécurité publics et aucun organisme indépendant n'a contrôlé les risques liés à la protection des données non plus – sans parler de la publication du code source. Pourquoi le canton de Berne n'édicte-t-il pas de directives à ce sujet ?

5. Comment s'assurer que les données sont bien supprimées de la banque de données centralisée et de celles des établissements de restauration ?
6. Comment s'assurer que les autres Directions et autorités n'utilisent pas à d'autres fins les données recueillies par le biais du traçage ?
7. Comment la sécurité de la banque de données centralisée est-elle garantie ? Quels audits sont-ils mis en œuvre ?
8. Quelles autres solutions que celle de la collecte centralisée de l'ensemble des coordonnées a-t-on envisagées ?

Motivation de l'urgence : la saisie des données est d'ores et déjà devenue une réalité dans les établissements de restauration.

Réponse du Conseil-exécutif

Question 1

Les prescriptions du canton de Berne en matière de sécurité de l'information et de protection des données (SIPD) ont été prises en compte dans le cadre du déploiement de la banque de données centralisée servant à la collecte des coordonnées. Cette banque de données a été conçue en collaboration étroite avec le Bureau pour la surveillance de la protection des données et lui a été soumise pour contrôle avant sa mise en service. Des tests de sécurité externes ont par ailleurs été réalisés.

Question 2

Pour des raisons tant techniques qu'organisationnelles, il n'est pas possible d'effectuer une recherche sur des personnes dans la banque de données (cf. réponse à la question 3).

Question 3

L'anonymisation des données n'est pas prévue, d'autant qu'elle serait contraire aux exigences liées au traçage des contacts. Les données personnelles sont en revanche pseudonymisées grâce à la solution de cryptage mise en œuvre, c'est-à-dire enregistrées dans la banque de données sans que l'on puisse établir un lien direct avec les personnes concernées.

Les données cryptées sont consultées dans le cadre d'un processus autorisé par du personnel médical après double contrôle et uniquement si un événement pertinent sur le plan épidémiologique survient. Dans un tel cas, les quelques collaboratrices et collaborateurs de l'équipe de traçage des contacts autorisés effectuent une recherche dans la banque de données en ciblant un établissement et une période donnée avant d'exporter vers l'application de traçage des contacts TRACY les données personnelles cryptées associées aux paramètres saisis. Ce n'est qu'au cours du processus d'exportation que celles-ci sont décodées pour ensuite apparaître en clair (c'est-à-dire sans cryptage) dans TRACY.

Question 4

Le canton de Berne est uniquement tenu d'assurer la protection des données contenues dans ses propres banques de données. Or, les applications de traçage des contacts sont proposées par des entreprises privées et souvent pour l'ensemble du territoire national. Tous les échanges sans exception réalisés depuis, vers et au sein de la banque de données centralisée du canton sont cryptés.

Question 5

Les données enregistrées dans la banque de données centralisée du canton sont automatiquement supprimées après 14 jours grâce à une méthode conçue selon la norme DIN 66398.

Question 6

La loi fédérale sur la protection des données (LPD) interdit le regroupement d'informations provenant de différentes banques de données conçues pour un usage spécifique sans le consentement des personnes concernées. A l'échelle cantonale, c'est l'article 3b, alinéas 1 et 2 de l'ordonnance COVID-19 qui est déterminant. Les autres Directions cantonales et les autres autorités ne disposent d'aucun droit d'accès à la banque de données.

Question 7

La banque de données a été conçue et mise en service en étroite collaboration avec le Bureau pour la surveillance de la protection des données. Des tests d'intrusion classiques ont été réalisés afin de garantir une sécurité des données maximale. Les documents relatifs à la SIPD exigés à l'article 17a de la loi cantonale sur la protection des données (LCPD) ont été élaborés et transmis au Bureau pour la surveillance de la protection des données pour un contrôle préalable. Ce dernier envisage en outre de mener dans les prochaines semaines son propre examen portant sur différents aspects relatifs à la protection des données (audit). Un entretien préliminaire a déjà eu lieu à ce sujet.

Question 8

Jusqu'au mois de mai 2021, les coordonnées étaient enregistrées de façon décentralisée et sans consigne précise quant à leur format, avec pour conséquence qu'en cas d'événement épidémiologique nécessitant la mise à disposition des données personnelles, l'équipe de traçage des contacts recevait des données de qualité très variable. Les données fournies étaient souvent incomplètes et de formats divers, ce qui impliquait un important travail de traitement de données pour l'équipe de traçage. Cette dernière a également été confrontée à des noms erronés ou farfelus (Hitler, Donald Duck...) voire à des données factices, ce qui témoignait du fait que les données n'avaient fait l'objet d'aucune validation. Les données devaient alors être demandées au cas par cas par l'équipe de traçage, parfois au prix de gros efforts pour joindre les personnes responsables dans les cafés, restaurants et hôtels. Ces démarches supplémentaires ont entraîné des retards, compliquant ainsi le travail de traçage des contacts. Si l'on ne voulait pas renoncer purement et simplement au traçage des contacts via une collecte des données, il était dès lors indispensable de mettre en place une solution centralisée. Dans ce contexte, le canton a aussi étudié la solution d'un prestataire privé, laquelle a été rejetée au profit de l'actuelle solution, justement pour des raisons liées à la protection des données.

Destinataire

– Grand Conseil