Appuyer la santé publique et bâtir la confiance des Canadiens : principes de protection de la vie privée et des renseignements personnels pour les applications de traçage des contacts et autres applications similaires

Déclaration commune des commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée[1]
7 mai 2020

En cette période de crise sanitaire liée à la COVID-19, la santé et la sécurité des Canadiens sont une préoccupation majeure. L'urgence de limiter la propagation du virus représente un défi de taille pour les gouvernements et les autorités de santé publique, qui cherchent des moyens d'utiliser des renseignements personnels pour obtenir un meilleur portrait de ce nouveau virus et de la menace mondiale qu'il représente, de même que pour les circonscrire.

Dans ce contexte, ils pourraient envisager davantage de mesures exceptionnelles, dont certaines porteront grandement atteinte à la vie privée et aux autres droits de la personne. Les choix effectués par nos gouvernements aujourd'hui quant à la manière d'atteindre les objectifs de santé publique tout en préservant nos valeurs canadiennes fondamentales, dont fait partie le droit au respect de la vie privée, façonneront l'avenir de notre pays.

Une des mesures présentement à l'étude ou déjà mises en œuvre à certains endroits au Canada et ailleurs dans le monde est le lancement d'applications mobiles comme outils de santé publique. Beaucoup de ces applications ont comme finalité soit le traçage des contacts, soit le fait d'informer les personnes qu'elles ont été en contact rapproché avec une personne testée positive à la COVID-19 ou jugée susceptible d'en être porteuse, afin d'éviter le plus possible la propagation du virus.

Les commissaires estiment qu'il est important d'émettre une déclaration commune aux Canadiens parce que ces applications soulèvent d'importants risques en matière de vie privée et de protection des renseignements personnels. Bien que les lois applicables sur la protection des renseignements personnels doivent être respectées, certaines d'entre elles ne prévoient pas un degré de protection adapté à l'environnement numérique, comme l'a mis en évidence une résolution commune diffusée l'automne dernier. C'est la raison pour laquelle nous invitons nos gouvernements respectifs, dans la mesure où ils prévoient utiliser des applications de traçage des contacts, à respecter à tout le moins les principes suivants :

- **Consentement et confiance :** L'utilisation des applications doit être volontaire. Cela sera indispensable pour bâtir la confiance du public. Cette confiance exigera également des gouvernements la démonstration d'un degré élevé de transparence et de responsabilité.

- **Conformité à la loi :** Les mesures proposées doivent avoir une assise juridique claire et le consentement doit être valable. Un consentement distinct doit être obtenu pour chacune

[1] Le Commissariat à l'information et à la vie privée de l'Alberta examine présentement une évaluation des facteurs relatifs à la vie privée au sujet de l'application ABTraceTogether, lancée récemment en Alberta, et fournira ses recommandations directement au gouvernement de l'Alberta.

des finalités de santé publique qui sont visées. Les renseignements personnels ne devraient pas être accessibles par les fournisseurs de service ou toute autre organisation et les utilisateurs ne doivent pas être contraints de les fournir à quiconque.

- **Nécessité et proportionnalité :** Les mesures doivent respecter les principes de nécessité et de proportionnalité, c'est-à-dire être fondées sur la science, nécessaires pour une fin particulière, adaptées à cette fin et susceptibles d'être efficaces. Pour déterminer si la mesure envisagée est justifiée dans les circonstances, les gouvernements devraient prendre en compte les critères suivants :

    - **Nécessité :** La fin ou les fins visées en matière de santé publique qui sous-tendent une mesure doivent reposer sur des données probantes et être définies avec un certain degré de précision. L'objectif est-il de notifier les utilisateurs et de les aviser de prendre certaines mesures? S'agit-il d'aider les autorités de santé publique à mieux comprendre la situation locale pour les besoins de l'affectation des ressources? L'objectif est-il autre?
    - **Proportionnalité :** La mesure devrait être conçue de manière à avoir un lien rationnel avec la ou les fins particulières à réaliser.
    - **Efficacité :** La mesure doit être susceptible d'être efficace pour atteindre le ou les objectifs déterminés.;
    - **Atteinte à la vie privée minimale :** Bien que l'option la moins intrusive pour la vie privée devrait être retenue et que seuls les renseignements nécessaires doivent être recueillis, lorsque cela est impossible ou que l'on ne peut faire la démonstration de l'ampleur de l'atteinte, les gouvernements devraient justifier clairement la quantité de renseignements personnels qu'ils souhaitent recueillir.

- **Finalité :** Les renseignements personnels doivent être utilisés uniquement pour les fins initialement prévues visant la protection de la santé publique et pour aucune autre fin.

- **Dépersonnalisation :** Les gouvernements devraient utiliser des données dépersonnalisées ou agrégées dans la mesure du possible, à moins que ce type de données ne permette pas d'atteindre l'objectif déterminé. Ils devraient prendre en compte le risque de réidentification, qui peut être plus élevé dans le cas des données de géolocalisation.

- **Durée limitée des mesures :** Les mesures exceptionnelles devraient être limitées dans le temps. Tout renseignement personnel recueilli pendant la période en cours devrait être détruit à la fin de la crise et l'application devrait être mise hors service.

- **Transparence :** Les gouvernements devraient indiquer clairement le fondement et les modalités se rapportant aux mesures exceptionnelles. Les Canadiens devraient être pleinement informés des renseignements qui seront recueillis, des utilisations prévues, des personnes ou organisations qui y auront accès, de l'emplacement où ils seront stockés, des mesures prévues pour les protéger pendant la période de conservation ainsi que du moment où ils seront détruits. Les gouvernements devraient réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) ou des analyses rigoureuses de protection de la vie privée, les soumettre à l'examen des commissaires à la protection de la vie privée et en publier de façon proactive un résumé en langage clair.

- **Responsabilité :** Les gouvernements devraient élaborer et rendre public un plan continu de suivi et d'évaluation de l'efficacité de ces initiatives et s'engager à publier le rapport d'évaluation dans un délai déterminé. Une surveillance exercée par un tiers indépendant – par exemple l'analyse de la mesure et l'examen de sa mise en œuvre par une autorité de contrôle en matière de protection de la vie privée – aidera à assurer la responsabilité et renforcera la confiance du public. La loi confère à certains commissaires à la protection de la vie privée le pouvoir de procéder à des vérifications indépendantes, mais il est souhaitable que les gouvernements confient ce mandat à l'ensemble des commissaires en prenant les moyens appropriés. Si l'efficacité de l'application ne peut être démontrée, alors celle-ci devrait être mise hors service et tout renseignement personnel recueilli devrait être détruit.

- **Garanties :** Des mesures de protection juridiques et techniques appropriées, y compris des dispositions contractuelles robustes conclues avec les développeurs d'applications, doivent être mises en place pour empêcher tout accès non autorisé aux renseignements personnels et toute utilisation de ces derniers à une fin autre que les finalités initiales liées à la santé publique. Les autorités doivent s'assurer que le public est conscient des risques et des menaces inhérents à cette technologie (p. ex. fraude en ligne ou maliciel).