

Compte rendu de l'Union nationale — Biométrie — septembre 2024

Préambule

Vous lierez dans ce document un extrait de l'allocution de M. Daniel Therrien, commissaire à la protection de la vie privée du Canada, prononcée le 14 octobre 2021 et du guide d'accompagnement pour les organismes publics et les entreprises de la Commission d'accès à l'information du Gouvernement du Québec. Ces deux extraits inspirent très bien le positionnement de l'Union nationale quant à la protection de la vie privée, à l'utilisation et la monétisation de nos données personnelles par les entreprises privées et à l'encadrement des nouvelles technologies. Voici un condensé des passages clés que nous désirons porter à l'attention du public.

Commissaire à la protection de la vie privée du Canada [1]

« On peut difficilement contester que les données occupent une place de plus en plus importante dans l'économie et que nous assistons au développement rapide de technologies axées sur les données.

Si la première révolution industrielle était celle de la vapeur, la quatrième est celle des données.

Un nombre croissant d'entreprises cherchent à monnayer nos données personnelles, tandis que les gouvernements envisagent diverses initiatives qui s'appuient sur la prise de décisions fondées sur les données, ainsi que sur un plus grand partage et une plus grande accessibilité de ces données. [...]

Or, l'importance croissante des données s'accompagne aussi de nouveaux risques pouvant avoir des répercussions importantes sur notre vie privée. Il est urgent de définir comment tirer avantage des données tout en respectant les valeurs démocratiques et les droits fondamentaux. [...]

Nous devrions tous nous soucier de la protection des renseignements personnels. [...]

La protection de la vie privée ne nuit pas à l'innovation économique ni aux intérêts du Canada en matière de sécurité nationale. En fait, des lois qui protègent adéquatement les renseignements personnels peuvent soutenir ces deux objectifs. [...]

En effet, nos sondages révèlent qu'une vaste majorité se soucie de la question et affirme être très préoccupée par leur incapacité à protéger leur droit à la vie privée, notamment contre la puissance croissante d'entreprises comme Facebook et Google, qui semblent en savoir davantage à notre sujet que nous en savons nous-mêmes.

Personne n'a su monnayer les données personnelles mieux que les géants de la technologie, qui sont derrière nos recherches dans Internet et nos comptes de médias sociaux. [...]

Notre objectif est de s'assurer que ces organismes utilisent les outils nécessaires à leur travail essentiel d'une manière conforme à la loi et respectueuse du droit à la vie privée. [...]

Je me dois de souligner que la technologie en soi n'est ni bonne ni mauvaise. Les nouvelles technologies peuvent, bien évidemment, offrir de grands avantages, mais elles comportent aussi des risques.

L'un des principaux objectifs de la réglementation est de créer un environnement dans lequel les individus ont l'assurance que leurs droits seront respectés.

Malheureusement, l'incapacité de nos lois à suivre le rythme a entraîné une crise de confiance au Canada, notamment en ce qui concerne les activités en ligne. [...]

Le scandale Facebook et Cambridge Analytica a mis en lumière les répercussions potentielles des plateformes en ligne sur la vie privée et l'intégrité des processus électoraux.

Par ailleurs, les atteintes à la sécurité des données ne cessent de gagner en importance et sont même devenues courantes, ce qui est scandaleux. Des atteintes touchent maintenant des centaines de milliers de personnes, des millions de personnes, voire des centaines de millions de personnes. Par exemple, le Commissariat a enquêté sur l'atteinte à la sécurité des données chez Desjardins, qui a compromis les renseignements personnels de près de 10 millions de Canadiens.

D'autres enquêtes menées récemment par le Commissariat ont, quant à elles, laissé entrevoir la menace que représente la surveillance de masse au Canada.

Je fais référence ici à notre enquête sur la société de technologie Clearview AI et à l'enquête connexe que nous avons menée sur la GRC.

Nous avons estimé que cette collecte de renseignements biométriques très sensibles, à l'insu des personnes concernées et sans leur consentement, est illégale. Des millions de personnes — dont la grande majorité ne commettra jamais de crime — se sont retrouvées dans une séance d'identification policière tous les jours, 24 heures sur 24, ce qui est tout à fait inacceptable.

Notre enquête sur la GRC a révélé que l'utilisation par le service de police de la technologie de reconnaissance faciale pour effectuer des centaines de recherches dans une base de données compilée illégalement par une entreprise commerciale constitue une violation de la Loi sur la protection des renseignements personnels.

Nous avons également constaté des lacunes graves et systémiques dans les politiques et les systèmes de la GRC concernant le suivi, l'identification, l'examen et le contrôle des nouvelles collectes de renseignements personnels au moyen de technologies innovantes. [...]

Au final, en ce qui concerne l'environnement numérique, nous ne pourrons réaliser de réels progrès pour accroître la confiance que lorsque nous adopterons des lois rigoureuses pour protéger les renseignements personnels. [...]

Des lois rigoureuses pour protéger les renseignements personnels permettent d'accroître la confiance à l'égard de nos systèmes et de nos institutions ; elles augmentent aussi la capacité de réagir aux menaces à la sécurité.

Pour certains, les mesures pour protéger la vie privée sont des contraintes qui limitent nos activités. Mais vues sous un autre angle, elles représentent plutôt une défense active. L'absence de lois efficaces sur la protection des renseignements personnels crée une vulnérabilité — les militaires parleraient d'une "cible inopinée". [...]

Les menaces peuvent provenir de n'importe où : des services de sécurité et de renseignement d'États hostiles, de pirates employant des rançongiciels, d'organisations criminelles ou d'autres agents perturbateurs. Elles visent les installations gouvernementales, les grandes sociétés pétrolières, et même les hôtels et les sites de rencontres. Des adversaires mettent peu de temps à relier les chaînes de données et à rassembler suffisamment de renseignements sensibles pour causer des dommages. [...]

Nous avons besoin d'un cadre fondé sur les droits qui reconnaît le droit fondamental à la vie privée. [...]

Il ne s'agit pas d'un problème abstrait. Le Conseil canadien des innovateurs considère qu'adopter une approche décousue, sans cohésion, à l'égard de la protection de la vie privée au Canada, c'est courir à la catastrophe. Du point de vue de l'innovation, il s'agit de la pire option. [...]

Cela est d'autant plus important dans un contexte où le gouvernement dépend de plus en plus de technologies mises au point par le secteur privé pour mener à bien ses activités. [...]

Cela ne signifie pas que cette technologie ne doit jamais être utilisée, mais que chaque fois qu'on y a recours, sa nécessité doit être établie. Le résultat recherché doit être directement lié à la mesure qui est prise et proportionnel au préjudice causé. [...]

Le Canada aspire à redevenir un chef de file mondial de la protection de la vie privée.

Nous croyons que les Canadiens méritent des lois fédérales en la matière qui soient fondées sur les droits. L'intégration d'un cadre fondé sur les droits permettrait de favoriser une innovation responsable et de susciter la confiance envers le gouvernement. Cela permettrait aux gens de participer pleinement et en toute confiance à l'économie numérique.

En adoptant une approche fondée sur les droits, le Canada deviendrait un chef de file dans ce domaine. Il montrerait la voie à suivre en définissant des lois sur la protection des renseignements personnels qui permettent d'atteindre les objectifs suivants : protéger la vie privée, stimuler le développement des affaires et l'innovation, et priver les États hostiles et les acteurs malveillants d'occasions qui pourraient entraîner des menaces à la sécurité nationale.

Comme société, nous devons projeter nos valeurs dans nos lois sur le numérique. Nos citoyens ne s'attendent à rien de moins de la part de leurs institutions publiques.

Un cadre solide à l'égard de la vie privée sera un atout pour bâtir un pays où priment protection, résilience et sécurité. Voilà un objectif auquel nous devrions tous contribuer. »

Guide d'accompagnement pour les organismes publics et les entreprises [2]

« La Commission constate, depuis plusieurs années, un recours accru à la biométrie tant dans le secteur privé que dans le secteur public. [...]

La popularité de la biométrie engendre néanmoins une certaine banalisation de ses implications en matière de protection des renseignements personnels. Si on la dit sécuritaire, on oublie cependant trop souvent que son utilisation présente des risques pour la vie privée des personnes. Le cadre légal qui s'applique à la biométrie est par ailleurs méconnu. [...]

Leur collecte constitue un degré d'intrusion élevé dans la vie privée des individus. [...]

Les renseignements biométriques revêtent un caractère particulièrement sensible. Ce sont des caractéristiques permanentes et distinctives, des identifiants uniques composés d'informations intimes. [...]

Ils peuvent susciter la convoitise d'acteurs malveillants. Ils doivent donc être protégés par des mesures de confidentialité et de sécurité fortes, qui tiennent compte notamment de leur quantité, de leur répartition et de leur support. [...]

Enfin, si la confidentialité de ces renseignements est compromise, des conséquences graves peuvent en résulter pour la personne concernée : s'il est possible de remplacer une carte magnétique, un numéro d'identification personnel (NIP) ou un mot de passe, on ne peut pas changer son visage ou ses empreintes digitales. [...]

La Loi sur le privé et la Loi sur l'accès prévoient que seuls les renseignements personnels nécessaires peuvent être recueillis. Cette règle ne peut être écartée en obtenant le consentement de la personne concernée. [...]

[Une] déclaration doit obligatoirement être faite à la Commission avant de commencer à utiliser la biométrie. [...]

Les obligations légales en vigueur au Québec quant à la biométrie s'appliquent à toute organisation souhaitant utiliser un système biométrique ou un procédé permettant de saisir des caractéristiques ou des mesures biométriques. [...]

Il importe qu'elles connaissent ces règles afin de bien conseiller leurs clients [d'éviter] de les induire en erreur. [...]

Les renseignements biométriques sont des renseignements personnels, c'est-à-dire des informations qui concernent un individu et permettent de l'identifier. Ils sont uniques, distinctifs et ils persistent dans le temps. [...]

la biométrie : physiques, comportementales ou biologiques, morphologiques, caméras thermiques, analyse de vidéo anonyme (AVA), bracelets de santé connectés, systèmes de reconnaissance des émotions, etc. C'est le cas pour les images (du visage, de l'iris, etc.) et les empreintes (doigts, contour de la main, voix, patron de frappe au clavier, etc.), qu'elles soient statiques (images ou empreintes fixes) ou dynamiques (images ou empreintes animées ou dotées d'une durée temporelle). [...]

C'est également vrai pour tout code (aussi appelé gabarit ou modèle), numérique ou autre, qui est dérivé de ces images à l'aide d'un algorithme. Dans la mesure où ce code, qui constitue une caractéristique ou une mesure biométrique, est conservé pour la reconnaissance ultérieure de la personne, il permet de l'identifier, puisqu'il est distinctif par nature. [...]

Il existe trois grandes catégories de biométrie :

- La biométrie morphologique est basée sur l'identification de traits physiques particuliers. Elle regroupe notamment, mais pas exclusivement, la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris de l'œil.
- La biométrie comportementale est basée sur l'analyse de certains comportements d'une personne, comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier, etc.

- La biométrie biologique est basée sur l'analyse des traces biologiques d'une personne, comme l'ADN, le sang, la salive, l'urine, les odeurs, etc. [...]

Le recours à la biométrie doit viser à résoudre une situation problématique, donc poursuivre un objectif important et légitime. [...]

La loi interdit d'exiger que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. Cela implique que :

- Vous devez obtenir le consentement valide et exprès de chaque personne ;
- Vous devez prévoir une solution alternative pour vérifier ou confirmer son identité, en cas de refus de la personne ou de retrait de son consentement ;
- Vous ne pouvez faire appel à des caractéristiques ou des mesures biométriques à l'insu de la personne concernée (saisies sans qu'elle en ait connaissance). [...]

Un consentement est qualifié d'"exprès" lorsqu'il est manifesté de manière explicite et sans équivoque. [...]

L'obtention du consentement ne vous libère pas de votre obligation de ne recueillir que les renseignements personnels nécessaires. [...]

Limité dans le temps : le consentement est donné pour une période temporelle définie. [...]

L'obligation d'obtenir le consentement exprès avant de pouvoir identifier une personne au moyen de caractéristiques ou de mesures biométriques implique que vous ne pouvez imposer cette façon de faire. Les personnes concernées ne devraient subir aucune pression ni aucun inconvénient par rapport à leur choix. Vous devez prévoir une solution alternative pour celles qui refuseront de consentir ou qui retireront leur consentement. Exemples de solutions alternatives :

- Système de cartes d'accès ;
- Utilisation de jetons uniques ;
- Utilisation d'un mot de passe ou d'un code d'identification.

La loi interdit que l'identification d'une personne ou la vérification de son identité se fasse en ayant recours à des caractéristiques ou à des mesures biométriques à son insu. Il s'agit d'une obligation apparentée à celle d'obtenir le consentement exprès. Cela implique que vous recueillez les caractéristiques et mesures biométriques directement auprès de la personne concernée.

Les renseignements biométriques que vous recueillez doivent être utilisés exclusivement pour atteindre l'objectif initial motivant la mise en place du système ou du procédé biométrique, à moins du consentement exprès de la personne concernée ou d'une exception prévue par la loi. Également, tout autre renseignement concernant une personne qui pourrait être découvert à partir des caractéristiques ou mesures biométriques ne peut pas être utilisé pour prendre une décision à son égard. [...]

Vous devez établir ces mesures en tenant compte du contexte dans lequel est implanté le système ou le procédé biométrique dont vous avez la responsabilité. La sécurité physique, informatique, logique et organisationnelle doit être assurée de différentes manières.

Afin de garantir un entreposage sécuritaire des renseignements biométriques et de préserver leur confidentialité, vos mesures devraient concerner notamment le format des données, le support de conservation, la localisation du serveur, les technologies d'amélioration de la confidentialité et la restriction de l'accès et de la communication à des tiers. [...]

Les renseignements biométriques que vous recueillez et entreposez ne doivent être accessibles qu'à un nombre restreint de personnes, soit celles dont les fonctions ou les mandats requièrent nécessairement l'utilisation de ces renseignements. Vous devez mettre en place un système de journalisation de façon à garder une trace des personnes qui consultent ou utilisent les renseignements biométriques, et ce, même si ces personnes sont des tiers ou des employés responsables de l'informatique au sein de votre organisation. Ce système devrait inclure l'exploitation des journaux de manière à détecter toute anomalie, dont un accès non autorisé, pour pouvoir intervenir rapidement et faire cesser cette intrusion.

Vous devez obtenir le consentement exprès de la personne concernée pour toute communication de ses renseignements biométriques à un tiers. »

Conclusion

À la lecture de ces deux documents, la nécessité de légiférer en matière d'utilisation des données biométriques pour assurer la protection de la vie privée et de la confidentialité de nos données personnelles apparaît clairement. Tant au Canada, qu'au Québec, les entreprises technologiques actuelles ont beau jeu. Notons aussi qu'un travail de sensibilisation et d'éducation de la population est nécessaire. N'hésitez pas à nous faire parvenir vos réflexions, vos actions et vos commentaires découlant de la lecture de ce compte rendu.

Jonathan Blanchette

Chef de parti

Union nationale

union.nationale.jonathan86@gmail.com

Bibliographie

[1] THERRIEN, Daniel. Allocution prononcée lors d'une série d'évènements virtuels organisés par le CIGI. Commissariat à la protection de la vie privée du Canada, Allocutions. 14 octobre 2021 [https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2021/sp-d_20211014/] (Consultée le 6 septembre 2024)

[2] GUIDE D'ACCOMPAGNEMENT. Biométrie : principes à respecter et obligations légales des organisations. Commission d'accès à l'information. Gouvernement du Québec. 21 septembre 2022 [https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_Biometrie_Organisations.pdf] (Consultée le 6 septembre 2024)