culture
Saguenay–Lac-Saint-Jean

COMPRENDRE LES RISQUES LÉGAUX ET ÉTHIQUES liés à la gestion de données

et être en mesure de mettre en place des stratégies de protection des données et de leurs usager·ères

Par Me Charlaine Bouchard

Apprentissage ciblé

Grâce à cette fiche, vous serez en mesure de comprendre les risques légaux et éthiques liés à la gestion de données, puis de mettre en place des stratégies de protection des données et de leurs usagers.

lexique

BIOMÉTRIE :

« La biométrie permet d'identifier ou d'authentifier une personne grâce à ses caractéristiques uniques. Il en existe trois grandes catégories :

- La biométrie morphologique est basée sur l'identification de traits physiques particuliers. Elle regroupe notamment 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, 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. »

CYBERSÉCURITÉ :

« Capacité, pour un système en réseau, de se protéger et de résister à des évènements issus du cyberespace et susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information qu'il contient. » .

INCIDENT DE CONFIDENTIALITÉ :

« Pour l'application de la ***Loi sur la protection des renseignements personnels dans le secteur privé***, on entend par "incident de confidentialité" : 1° l'accès non autorisé par la loi à un renseignement personnel; 2° l'utilisation non autorisée par la loi d'un renseignement personnel; 3° la communication non autorisée par la loi d'un renseignement personnel; 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement. »

RENSEIGNEMENTS PERSONNELS :

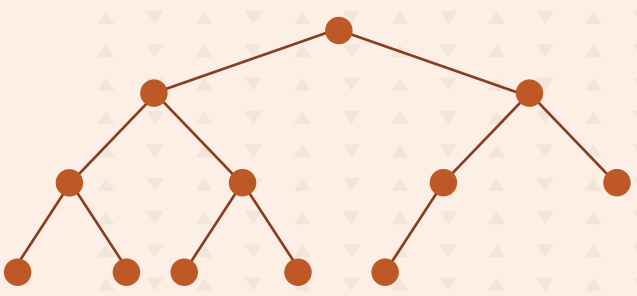
« Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée. »

Pour mieux comprendre

La réforme de la ***Loi sur la protection des renseignements personnels dans le secteur privé*** renforce les obligations légales des organisations d'assurer la protection des renseignements personnels. Par exemple, elle instaure un tout nouveau régime de notification des incidents de confidentialité aux personnes concernées.

Cybersécurité

Les organisations doivent prendre les mesures de sécurité appropriées et raisonnables pour protéger les renseignements personnels en tenant compte notamment de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. De cette manière, plus un renseignement est sensible, plus les mesures de sécurité doivent être importantes.



Incidents de confidentialité

Les organisations ayant des « motifs de croire » qu'un incident de confidentialité a eu lieu se doivent de prendre des « mesures raisonnables pour diminuer le risque qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ». En pratique, cela signifie que les organisations doivent prendre toutes les mesures appropriées et raisonnables afin de prévenir le préjudice pouvant être causé aux individus à la suite de l'incident, et ce, sans égard au niveau de gravité du risque.

Évaluation du risque de préjudice sérieux

Tous les incidents de confidentialité doivent faire l'objet d'un processus d'évaluation du « risque de préjudice sérieux » afin de déterminer si l'incident en question doit être notifié à la Commission d'accès à l'information (CAI) et aux personnes concernées.

Pour évaluer le niveau de gravité du risque du préjudice, voici quelques facteurs à prendre en considération :

- **La sensibilité des renseignements en cause** *:* Les renseignements qui, en raison de leur nature (ex. : médicale, biométrique ou autrement intime) ou du contexte de leur utilisation, font croître le risque de préjudice;

- **Les conséquences appréhendées de leur utilisation** *:* Par exemple, si les renseignements compromis sont susceptibles d'être utilisés pour commettre une fraude ou un vol d'identité;

- **La probabilité qu'ils soient utilisés à des fins préjudiciables.**

Notification des incidents

Si l'organisation juge que l'incident présente un risque de préjudice sérieux pour les individus touchés, elle doit aviser la Commission d'accès à l'information ainsi que tout individu concerné par l'incident, à défaut de quoi la Commission pourra lui ordonner de le faire.
Aucun délai n'est prévu pour la notification des incidents, mais celle-ci doit se faire avec « diligence », c'est-à-dire que la notification doit être faite avec soin et empressement.
De plus, les organisations doivent tenir un registre des incidents de confidentialité, dont une copie doit être transmise à la Commission sur demande de celle-ci.

Biométrie

Les caractéristiques ou les mesures biométriques issues d'analyses sont considérées comme des renseignements personnels, aussi appelés renseignements biométriques. Leur format peut être brut (image, visage, iris ou empreinte) ou codé (code ou gabarit chiffré). D'ailleurs, à compter du 22 septembre 2023, ***la Loi sur l'accès à l'information*** et la ***Loi sur la protection des renseignements personnels dans le secteur privé*** indiqueront explicitement que les renseignements biométriques sont des renseignements sensibles.
En raison du caractère sensible de ces données, les organisations devront se soumettre à certaines obligations, dont :

- **Déclarer le système ou le procédé biométrique**: à la Commission d'accès à l'information avant la mise en service du système ou procédé biométrique;
- **Obtenir le consentement valide et exprès** des personnes concernées et prévoir un autre moyen d'identification en cas de refus;
- **Respecter la finalité de la collecte :** Les renseignements biométriques recueillis doivent être utilisés exclusivement pour l'objectif initial, à moins d'obtenir le consentement exprès de la personne concernée;
- **Mettre en place des mesures de confidentialité et de cybersécurité:** Afin de garantir un entreposage sécuritaire des renseignements biométriques et de préserver leur confidentialité, les mesures mises en place par les organisations devraient concerner notamment le format des données, le support de conservation, la localisation du serveur, les technologies d'amélioration de la confidentialité ainsi que la restriction de l'accès et de la communication à des tiers.

Si les données sont stockées à l'extérieur du Québec, les organisations devront s'assurer que les renseignements ne seront pas utilisés à des fins incompatibles avec l'objectif de la collecte, ni communiqués sans le consentement des personnes concernées, sauf dans les cas prévus par la loi.

De plus, dès 2023, les organisations devront procéder à une évaluation des facteurs relatifs à la vie privée afin de s'assurer que la protection des renseignements personnels est adéquate. Notez que l'utilisation du terme à « l'extérieur du Québec » s'applique aussi à l'échange de renseignements personnels d'une province à l'autre.

- **Détruire de manière sécuritaire et définitive**: Lorsque l'objectif associé à la collecte des caractéristiques ou des mesures biométriques a été atteint, les organisations ont l'obligation de les détruire. Puisque ces renseignements personnels sont sensibles, il est essentiel d'utiliser une méthode de destruction définitive et irréversible (ex. : une technique d'anonymisation qui ne permet plus, de manière définitive, de relier un renseignement à un individu);
- **Assurer les droits d'accès et de rectification :** Toute personne a un droit d'accès aux renseignements personnels qui la concernent et qui sont détenus par une organisation. Elle est également en droit de demander la rectification de ces renseignements.

Exemples d'usage concret

1. De grands projets ont été réalisés au Québec en cybersécurité. Parmi eux, mentionnons la création de Qohash, une entreprise qui propose des solutions de cybersécurité.

2. À l'été 2022, le gouvernement du Québec a accordé une aide financière de plus de 3,5 M$ à In-Sec-M, une organisation québécoise spécialisée dans la cybersécurité, pour un projet qui vise entre autres à renforcer la protection des renseignements personnels dans les PME québécoises.

Conseils d'experte

- Faites une évaluation des facteurs relatifs à la vie privée avant tout projet impliquant des données biométriques.
- Élaborez et mettez à jour la politique de gestion des incidents de l'organisation de manière à y inclure les nouvelles obligations.

RÉFÉRENCES SUPPLÉMENTAIRES

- Les nouvelles exigences des organisations quant à la protection des renseignements personnels ainsi que leur entrée en vigueur respective sont très bien expliquées dans le ***Guide de conformité pour les entreprises*** créé par le cabinet Borden Ladner Gervais:
  https://www.blg.com/fr/insights/2021/11/quebec-privacy-law-reform-a-compliance-guide-for-organizations;

- Le gouvernement du Canada a mis en place le Centre canadien pour la cybersécurité. Vous y trouverez des conseils, des avis et beaucoup d'informations spécialisées pour le grand public, les PME, les grandes organisations et infrastructures, les institutions gouvernementales ainsi que le milieu universitaire : **https://cyber.gc.ca/fr.**

BIBLIOGRAPHIE

Code civil du Québec (RLRQ), c. CCQ-1991 : à jour au 1er juin 2022, [Québec], Éditeur officiel du Québec, 2022.
https://www.canlii.org/fr/qc/legis/lois/rlrq-c-ccq-1991/derniere/rlrq-c-ccq-1991.html?resultIndex=1

Commission d'accès à l'information. (2022). ***Biométrie.*** Gouvernement du Québec.
https://www.cai.gouv.qc.ca/biometrie

Gratton, É., Henry, E., Joli-Cœur, F., Du Perron, S., Jarvie, M., Gauthier, J., Nagy, A., El Khoury, D.-N., Hémond, A. et Labasi-Sammartino, C. (2021). ***Réforme des lois québécoises en matière de protection des renseignements personnels : guide de conformité pour les entreprises.*** Borden Ladner Gervais LLP.
https://www.lexology.com/library/detail.aspx?g=a4a72845-5dc9-4d69-b006-9bf33f9b3237

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ), c. 25 : à jour au 22 septembre 2021, [Québec], Éditeur officiel du Québec, 2021.
https://www.canlii.org/fr/qc/legis/loisa/lq-2021-c-25/derniere/lq-2021-c-25.html

Loi sur l'accès à l'information (LRC), c. A-1 : à jour au 2 novembre 2022, [Canada], 1985.
https://laws-lois.justice.gc.ca/fra/lois/a-1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ), c. A-2.1 : à jour au 1er juin 2022, [Québec], Éditeur officiel du Québec, 2021.
https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html

Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ), c. P-39.1 : à jour au 1er juin 2022, [Québec], Éditeur officiel du Québec, 2021.
https://www.canlii.org/fr/qc/legis/lois/rlrq-c-p-39.1/derniere/rlrq-c-p-39.1.html

Littératie sur la donnée - De l'éveil au leadership est un projet de Culture Saguenay–Lac-St-Jean financé par

Conseil des Arts du Canada
Canada Council for the Arts
Culture et Communications Québec