

Transparence - Technologies d'identification, de localisation ou de profilage, exceptions

Modifications à la Loi sur la protection des renseignements personnels dans le secteur privé du Québec
Articles 8.1, 8.2

Introduction

Le 22 septembre 2021, le Québec a adopté la [*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*](#) (2021, chapitre 25) (la « Loi ») qui met à jour les lois sur la protection des renseignements personnels dans le secteur public et dans le secteur privé. Les dispositions de la Loi entrent en vigueur sur une période de 3 ans.

Ce document a été créé par des sommités canadiennes en matière de protection des renseignements personnels, en collaboration avec des associations industrielles nationales et régionales. Nous pensons qu'il est important d'adopter une approche harmonisée des lois sur la protection des renseignements personnels dans toutes les juridictions canadiennes afin que les règles soient compréhensibles pour les particuliers et les entreprises. L'interprétation des lois sur la protection des renseignements personnels doit être pragmatique, raisonnable et axée sur les résultats pour les particuliers et la mise en œuvre pour les entreprises. Dans cet esprit, nous avons élaboré des conseils qui nous semblent appropriés pour interpréter les dispositions les plus complexes de la Loi.

Ce document peut être partagé et utilisé par les entreprises. Il ne s'agit pas d'un avis juridique, mais de recommandations, de pratiques exemplaires à l'intention des entités qui souhaitent se conformer à la Loi avant que le gouvernement ou la Commission d'accès à l'information (la « CAI ») ne fournisse des règlements ou des directives supplémentaires. Nous encourageons les entreprises à suivre les développements de la CAI et des autorités gouvernementales sur ces sujets et ceux liés à la Loi.

Transparence — Technologies d'identification, de localisation ou de profilage

Lorsqu'une organisation utilise des renseignements personnels en ayant recours à des technologies d'identification, de localisation et/ou de profilage, la Loi modificatrice prévoit de nouvelles exigences de notification afin d'améliorer la transparence pour les individus.

L'article 8.1 stipule que :

- Les organisations doivent informer les personnes au préalable de toute collecte de renseignements personnels en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage.

- Les organisations doivent également informer les personnes des moyens offerts pour activer ces fonctions.
- Le « profilage » est défini comme « la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne ».
- Les termes « identifier » et « localiser » ne sont pas explicitement définis dans la loi ; toutefois, ces termes pourraient être raisonnablement définis comme suit :
 - « Identifier » signifie associer des renseignements anonymes ou pseudonymes à une personne physique spécifique.
 - « Localiser » signifie déterminer l'emplacement géographique d'une personne physique avec une précision raisonnable, par exemple en identifiant les coordonnées de longitude/latitude, ou en déterminant qu'un utilisateur se trouve dans un pâté de maisons. Dans le cours normal des choses, « localiser » n'inclut pas la déduction qu'un utilisateur soit situé dans un pays ou une zone municipale particulière, ce qui peut être déduit par l'adresse IP/le fournisseur de services Internet.

Vous trouverez ci-dessous une brève description des nouvelles exigences ainsi que des recommandations :

1. Utilisation de renseignements personnels pour les technologies d'identification, de localisation et de profilage

Une organisation qui recueille des renseignements personnels à l'aide de technologies dotées de fonctions permettant d'identifier, de localiser ou de profiler une personne doit informer cette dernière de l'utilisation de ces technologies et des moyens offerts pour activer ces fonctions.

Si vous répondez oui aux questions suivantes, vous avez l'obligation d'informer.

a. Utilisez-vous une technologie comprenant des fonctions permettant d'identifier, de localiser ou de profiler un individu ?

- **Identification d'un individu** : Utilisez-vous une technologie qui permet d'identifier un individu (non pas de manière pseudonyme, mais en tant que personne physique ou identifiable) ?
- **Localisation d'un individu** : Suivez-vous l'emplacement géographique d'un individu (c'est-à-dire où il se trouve ou où il a été récemment) ?
 - Tenez compte de l'exactitude et de la précision. Plutôt que de déduire l'emplacement, tentez-vous d'identifier avec précision l'emplacement

réel» d'une personne? Essayez-vous d'identifier son emplacement précis (par exemple, un coin de rue), plutôt que son emplacement approximatif (par exemple, une ville ou un pays)?

- **Profilage d'un individu** : Analysez-vous ou préisez-vous les caractéristiques ou le comportement d'un individu en vous basant sur des renseignements personnels?
 - La Loi modificatrice donne une définition très large du « profilage », qui englobe tout traitement de renseignements personnels effectué pour évaluer les caractéristiques d'un individu dans tout contexte et à toute fin — en ligne et hors ligne.
 - Le plus souvent, le profilage vise à mieux atteindre et servir les clients, notamment pour
 - Proposer des publicités plus pertinentes et ciblées ou tarifier des produits ou services en fonction des intérêts, de la fiabilité, du comportement ou de la localisation déduits.
 - Suggérer des produits plus pertinents en fonction de l'historique d'achat, de la situation économique, des préférences ou des intérêts d'une personne.

L'obligation d'informer ne concerne pas uniquement les clients potentiels et actuels, mais toute personne qui interagit avec votre organisation, y compris les visiteurs du site web et les employés.

Lorsque la collecte de renseignements personnels se fait pour le compte d'un tiers, c'est l'utilisateur final qui doit veiller au respect de toutes les exigences prévues par la loi.

b. Utilisez-vous des renseignements personnels ?

Les exigences s'étendent à l'utilisation des renseignements personnels, mais ne s'appliquent pas au traitement des renseignements anonymisés ou agrégés.

2. Obligation d'informer les individus

Dès lors que vous confirmez que votre organisation collecte des renseignements personnels à l'aide d'une technologie comportant des fonctions permettant d'identifier, de localiser ou de profiler une personne, il existe une nouvelle obligation d'informer cette dernière.

a. Comment et quoi informer

- Les organisations doivent être transparentes et utiliser un langage clair et simple.

- Informer peut se faire par différents moyens et les organisations peuvent adopter une approche à plusieurs niveaux, selon ce qui est approprié et raisonnable (par exemple, des informations générales dans une politique de confidentialité, des conditions générales, un site web, une FAQ, et des informations plus spécifiques sur des formulaires ou dans d'autres communications directes comme un avis « juste à temps » ou une fenêtre pop-up).
- La notification doit toujours être raisonnablement proéminente. Le niveau de proéminence et de détail doit dépendre des circonstances, notamment des facteurs suivants :
 - L'impact de l'identification, de la localisation ou du profilage sur le consommateur.
 - Les attentes raisonnables de la personne; plus une activité est inattendue, plus une organisation doit prendre des mesures pour la porter à l'attention de la personne.
 - [Les associations peuvent inclure des exemples spécifiques au secteur, à l'industrie ou à la profession, le cas échéant].
- Soyez clair avec les clients sur les fonctions qui sont activées par défaut (par exemple, « En téléchargeant cette application, vous allez être profilé, ce qui signifie.... »). Voir la section 3 ci-dessous.
- Les organisations doivent également envisager les cas où un *opt-in* peut être approprié. Voir la section 4 ci-dessous.

b. Quand informer

- Selon les circonstances, les organisations devraient informer les personnes au moment de la collecte des renseignements personnels.

3. Informer les individus des moyens d'activer les fonctions

Les organisations doivent informer les personnes des circonstances dans lesquelles il existe des moyens offerts pour activer les fonctions décrites ci-dessus (c'est-à-dire les fonctions qui permettent d'identifier, de localiser ou de profiler une personne).

En plus d'être transparentes avec les clients quant aux fonctions activées par défaut, les organisations doivent être claires quant aux choix dont disposent les personnes pour choisir expressément d'activer les fonctions conformément à leurs préférences.

- Les organisations devraient envisager de proposer des options pour activer des fonctions qui optimiseraient les performances et la personnalisation, plutôt que des fonctions qui sont nécessaires pour fournir un produit ou un service.

- Par exemple, un site ou une application de rencontres pourrait donner aux utilisateurs la possibilité d'activer le suivi de la localisation afin d'améliorer l'expérience d'une personne en lui montrant les autres utilisateurs à proximité. Cette fonction permettrait d'optimiser la prestation du service dans son ensemble, au lieu d'être essentielle.

4. Envisager les cas où un *opt-in* est approprié

Au cas par cas, les organisations devraient envisager les cas où un consentement exprès peut être approprié. Voir les orientations séparées sur le consentement.

Les organisations doivent procéder à une évaluation contextuelle des attentes raisonnables des personnes concernées, ainsi que de tout risque de préjudice, pour déterminer si le consentement doit être requis (ou si une exception au consentement s'applique).

- Tenir compte des attentes raisonnables d'une personne : Par exemple, compte tenu de ce qui pourrait être de véritables problèmes de sécurité, le consentement peut être requis pour la localisation précise dans le contexte des applications de médias sociaux. Le consentement devrait également être requis pour tout suivi de localisation lorsqu'une application n'est pas activement utilisée.
- L'identification et le profilage devraient nécessiter un consentement préalable pour toute activité susceptible d'être associée à ou de révéler l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'état de santé, la vie sexuelle ou l'orientation sexuelle.

Lorsque les renseignements personnels sont sensibles (art. 12 al. 4), ainsi que lorsque des renseignements médicaux, biométriques ou « autrement intimes » sont utilisés, le consentement explicite est requis (par exemple, l'utilisation d'une empreinte digitale ou d'une image faciale, ou le suivi du rythme cardiaque d'une personne). Certains types de profilage sont déjà soumis à des restrictions réglementaires distinctes (par exemple, les rapports sur le crédit à la consommation), qui prévalent sur toute orientation donnée.