EXPLORER LES ZONES INTERDITES : UN APERÇU DES ORIENTATIONS PUBLIÉES PAR LE COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA LIÉES AUX PRATIQUES INACCEPTABLES

Publié le 30 décembre, 2024

Catégories: Perspectives, Publications

La protection des renseignements personnels est la pierre angulaire du droit à la vie privée au Canada. En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** »), lorsque les organisations recueillent, utilisent ou communiquent des renseignements personnels, elles doivent le faire à des « fins acceptables ». Le Commissariat à la protection de la vie privée du Canada (« **Commissariat** ») a identifié plusieurs « zones interdites »[1], c'est-à-dire des pratiques qu'une personne raisonnable considérerait comme inacceptables dans les circonstances.

Le présent bulletin examine les zones interdites identifiées par le Commissariat et de nouvelles zones interdites liées à l'utilisation de systèmes d'intelligence artificielle générative (« **IA générative** »).

1. Qu'est-ce qu'une zone interdite?

En vertu du paragraphe 5(3) de la LPRPDE, une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Le critère de la personne raisonnable est évalué de manière objective en fonction du contexte plutôt que de manière subjective en fonction de l'expérience de l'individu[2]. C'est pourquoi l'obtention du consentement des personnes ne dispense pas une organisation de son obligation d'utiliser les renseignements personnels à des fins acceptables.

L'utilisation à des fins acceptables sert de rempart pour garantir que les pratiques d'une organisation en matière de protection de la vie privée restent dans les limites des attentes de la société. Lorsqu'elles interprètent le paragraphe 5(3), les organisations doivent s'efforcer de trouver un équilibre entre le droit à la vie privée et les besoins légitimes de l'organisation. Cet exercice de « pondération des droits » est essentiel pour déterminer quelles fins peuvent être acceptables (ou inacceptables) en vertu de la LPRPDE.

Dans les orientations publiées par le Commissariat concernant l'interprétation du paragraphe 5(3) de la

LPRPDE, le Commissariat a identifié certaines pratiques qu'une « personne raisonnable » jugerait inappropriées, qui constituent des zones interdites[3].

En classant certaines pratiques en tant que zones interdites, le Commissariat envoie un message clair aux organisations : ces pratiques ne sont pas acceptables en vertu des lois canadiennes sur la protection de la vie privée, même si elles sont menées de manière peu intrusive ou si le consentement de la personne a été obtenu.

Voici un aperçu des six zones interdites établies par le Commissariat :

2. Les zones interdites en vertu de la LPRPDE

a. La collecte, l'utilisation ou la communication de renseignements personnels à des fins contraires aux lois canadiennes

La première zone interdite concerne la collecte, l'utilisation ou la communication de renseignements personnels à des fins contraires aux règles de droit, aux lois ou aux règlements. Les organisations sont censées connaître et respecter toutes les lois canadiennes applicables à leurs activités. Les pratiques qui enfreignent les lois canadiennes ne peuvent évidemment pas être menées à des « fins acceptables » et sont considérées comme illégales en vertu de la LPRPDE.

Ces activités peuvent notamment inclure celles qui sont explicitement illégales, comme la fraude ou l'usurpation d'identité, ou les pratiques contraires aux lois en matière de vie privée, comme les lois sur les renseignements concernant le consommateur ou les lois en matière de discrimination.

b. Le profilage ou la catégorisation inacceptables

La deuxième zone interdite est la collecte, l'utilisation ou la communication de renseignements personnels à des fins de profilage ou de catégorisation, pouvant entraîner des violations de la législation sur les droits de la personne. Le profilage et la catégorisation sont devenus de plus en plus courants à l'ère des mégadonnées. Si le profilage peut fournir des renseignements précieux pour personnaliser les services ou améliorer la prise de décision au sein de l'organisation, son utilisation abusive peut conduire à des pratiques illégales.

Le profilage ou la catégorisation qui conduit à une discrimination fondée sur des motifs interdits, notamment la race, le sexe, l'âge, la religion ou un handicap, constitue une violation de la législation sur les droits de la personne et sera toujours inacceptable en vertu de la LPRPDE. Même lorsque le profilage ne viole pas la législation sur les droits de la personne, les organisations doivent se montrer prudentes, car le profilage donnant lieu à un traitement injuste ou contraire à l'éthique pourrait être jugé inacceptable.

c. La collecte, l'utilisation ou la communication de renseignements personnels à des fins qui causent ou

sont susceptibles de causer un préjudice grave à des individus

La troisième zone interdite établie par le Commissariat concerne la collecte, l'utilisation ou la communication de renseignements personnels à des fins qui causent ou sont susceptibles de causer un préjudice grave à des individus; une personne raisonnable considérerait cette pratique comme inacceptable.

Le terme « préjudice grave »[4] fait référence à une série de conséquences négatives qui peuvent avoir un impact durable et grave sur les individus, notamment:

- les lésions corporelles, comme des blessures physiques résultant d'atteintes à la vie privée, ou la traque rendue possible par la fuite de données de localisation,
- l'humiliation, le dommage à la réputation ou aux relations, comme la divulgation de renseignements personnels sensibles, de photographies intimes ou de dossiers médicaux qui peuvent ternir l'image d'une personne ou mettre à mal ses relations personnelles,
- la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles, comme la diffusion de renseignements inexacts ou nuisibles susceptibles d'influencer les décisions d'embauche ou les perspectives de carrière d'une personne,
- la perte financière ou l'usurpation d'identité, comme l'utilisation non autorisée de renseignements personnels pour accéder à des comptes bancaires, commettre des fraudes ou effectuer des achats frauduleux,
- les effets négatifs sur le dossier de crédit, comme l'utilisation inappropriée des données de crédit entraînant le refus de prêts ou d'autres services financiers et
- le dommage aux biens ou leur perte, comme l'exploitation de renseignements personnels dans le but de commettre des vols ou des actes de vandalisme.

Le Commissariat considère qu'une personne raisonnable estimerait inacceptable que les organisations obligent un individu à assumer un risque disproportionné de préjudices graves en contrepartie de produits ou de services. Bien que les consommateurs fassent souvent des compromis au chapitre de leur vie privée à des fins de commodité, les organisations doivent s'assurer qu'elles n'exposent pas les individus à un risque élevé de préjudices graves.

d. La publication non autorisée de renseignements personnels sensibles

La quatrième zone interdite est la publication non autorisée de renseignements personnels en ligne ou d'autres renseignements sensibles, principalement dans le but de réclamer un paiement aux individus pour retirer ces renseignements. Le Commissariat estime que le fait de tirer profit de la détresse d'une personne ou de sa crainte de voir sa réputation entachée est clairement contraire aux lois canadiennes sur la protection de

la vie privée.

La Cour fédérale du Canada a confirmé la position du Commissariat dans une affaire concernant une organisation qui republiait des documents judiciaires accessibles au public et demandait à des particuliers de payer pour les retirer[5]. Bien que les documents aient été publics au départ, l'organisation a facilité leur accès et a demandé à des particuliers de payer pour les retirer. Cette pratique a été jugée inacceptable en vertu de la LPRPDE.

e. La recherche de mots de passe des comptes de médias sociaux pour la sélection des employés

La cinquième zone interdite concerne la pratique consistant à exiger des mots de passe des comptes de médias sociaux dans le cadre de la gestion des relations avec les employés ou du processus de sélection des candidats à l'emploi. Les employeurs procèdent souvent à des vérifications d'antécédents afin d'évaluer les qualifications, l'aptitude et le caractère d'un candidat. Si ces vérifications peuvent inclure un examen des renseignements accessibles au public, le fait d'exiger l'accès à des zones de leurs comptes de médias sociaux protégées au moyen d'un mot de passe dépasse les limites sur le plan éthique et juridique.

La relation de travail est intrinsèquement déséquilibrée, les employeurs disposant d'un plus grand pouvoir de négociation. Lorsque les employeurs demandent l'accès aux médias sociaux privés, les candidats et les employés peuvent se sentir obligés de s'y conformer par crainte de perdre une opportunité d'emploi ou leur poste actuel. En fin de compte, le Commissariat indique que la pratique consistant à demander les mots de passe des médias sociaux est très invasive et est inacceptable en vertu de la LPRPDE.

f. La surveillance à l'aide de l'appareil de l'individu

La sixième zone interdite concerne la surveillance, secrète ou ouverte, de l'appareil d'une personne au moyen des fonctions audio ou vidéo. Le Commissariat considère que cette pratique représente l'une des violations les plus intrusives de la vie privée.

La surveillance des appareils fait généralement référence à l'utilisation non autorisée ou excessive des fonctions intégrées d'un appareil, comme l'écoute des conversations via le microphone de l'appareil, l'activation de l'appareil photo pour capturer des images ou des vidéos, ou le suivi de l'activité de l'écran de l'appareil, comme l'historique de navigation ou l'utilisation d'applications.

L'essor des appareils de l'internet des objets (IdO) a introduit de nouveaux défis dans ce domaine. Les appareils tels que les haut-parleurs intelligents, les caméras connectées et la technologie portable sont de plus en plus intégrés dans la vie quotidienne. Ces appareils sont souvent dotés de fonctions qui peuvent être exploitées à des fins de surveillance, ce qui brouille la frontière entre la fonctionnalité légitime et l'atteinte à la vie privée.

Le Commissariat a constaté que l'utilisation de logiciels espions ayant permis à plusieurs entreprises de location avec option d'achat de retrouver secrètement des ordinateurs portables manquants en recueillant des frappes, des captures d'écran, des photographies prises au moyen de la caméra Web et d'autres renseignements violait les lois sur la protection de la vie privée[6], car ce type de surveillance entraînait des préjudices largement disproportionnés par rapport à l'objectif commercial visé, à savoir la récupération des ordinateurs portables disparus.

3. L'émergence de zones interdites liées à l'IA générative

L'IA générative est une technologie transformatrice qui a le potentiel d'améliorer la créativité, la productivité et l'innovation. Toutefois, son utilisation abusive peut entraîner des risques importants en matière d'atteinte à la vie privée. Dans les Principes pour des technologies de l'intelligence artificielle (IA) générative responsables, dignes de confiance et respectueuses de la vie privée (« **Principes IAGen** »), co-édités par tous les régulateurs de la vie privée du Canada, les régulateurs ont identifié plusieurs *nouvelles* zones interdites potentielles liées à l'utilisation de l'IA générative[7]:

a. La création de contenu à des fins malveillantes

L'IA générative peut être utilisée à mauvais escient pour produire des contenus à des fins malveillantes ou nuisibles qui portent atteinte à la vie privée et sapent la confiance dans les interactions numériques. Par exemple :

- L'IA générative est utilisée pour générer des vidéos ou des images qui manipulent l'image réelle d'une personne à des fins malveillantes (communément appelées « deepfakes »), telles que la diffusion de faux renseignements sur une personne, l'usurpation de son identité ou la création et la diffusion d'images intimes sans son consentement.
- L'IA générative est utilisée pour falsifier des données biométriques, telles que les caractéristiques faciales ou vocales, afin d'obtenir un accès non autorisé à des systèmes sécurisés ou de contourner des systèmes d'authentification.

b. L'utilisation de robots conversationnels à des fins manipulatrices

Les chatbots alimentés par l'IA générative peuvent simuler de manière convaincante des conversations humaines, ce qui en fait des outils précieux pour les opérations de service à la clientèle et pour susciter l'engagement des clients. Cependant, lorsqu'ils sont mal utilisés, ils peuvent devenir des instruments de manipulation. Par exemple, l'utilisation de chatbots conçus pour inciter les individus à révéler des informations personnelles ou sensibles sous le couvert d'une interaction légitime, pour tromper les individus sur l'objectif de l'interaction ou pour pousser un individu à prendre une décision qu'il n'aurait pas prise autrement, pourrait

constituer une violation des lois sur la protection de la vie privée.

c. Le contenu faux ou diffamatoire

L'IA générative peut également être utilisée pour produire du contenu faux ou diffamatoire. Par exemple, l'IA générative pourrait être utilisée pour générer des textes ou des contenus audio attribués à une personne et portant atteinte à sa réputation, ou pour produire des contenus présentant une personne sous un faux jour, susceptible de l'humilier publiquement ou de lui causer de la détresse.

4. À retenir

Alors que le paysage numérique continue d'évoluer, le Commissariat a identifié plusieurs pratiques inacceptables liées à la collecte, l'utilisation et le traitement des renseignements personnels, ce qui constitue un outil essentiel pour les organisations confrontées à la complexité du paysage juridique canadien en matière de protection de la vie privée. En évitant les fins inacceptables ou les « zones interdites », les organisations peuvent démontrer leur engagement à respecter la vie privée des personnes, à favoriser la confiance et à sauvegarder leur réputation à l'ère des mégadonnées.

Les organisations doivent rester vigilantes, s'adapter et adopter une approche raisonnée, en veillant à ce que leurs pratiques respectent non seulement les exigences de la loi, mais aussi les attentes d'une société raisonnable et informée. Au-delà de la conformité, les organisations ont une responsabilité sociale dans le maintien de l'intégrité de l'économie numérique et la protection des droits fondamentaux de tous les Canadiens.

[1] Commissariat à la protection de la vie privée du Canada, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)* (mai 2018). **[Guide des zones interdites]**
[2] *Canada (Privacy Commissioner)* v. *Facebook, Inc.*, 2024 FCA 140, aux par. 60-63.
[3] *Guide des zones interdites*.
[4] LPRPDE, par. 10.1(7).
[5] Commissariat à la protection de la vie privée du Canada, *Rapport de conclusions d'enquête en vertu de la LPRPDE no 2015-002*.
[6] Commissariat à la protection de la vie privée du Canada, *Rapport de conclusions en vertu de la LPRPDE no 2013-016*.
[7] Commissariat à la protection de la vie privée du Canada, *Principes pour des technologies de l'intelligence artificielle (IA) générative responsables, dignes de confiance et respectueuses de la vie privée* (décembre2023).

Par Amir Kashdaran et Robbie Grant

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt obtenir des conseils juridiques précis.