LPRPDE – COMMENT OBTENIR UN CONSENTEMENT « VALABLE », ET QUAND LE CONSENTEMENT N'EST PAS JUGÉ ACCEPTABLE

Publié le 30 mai, 2020

Catégories: Perspectives, Publications

Le 24 mai 2018, le Commissariat à la protection de la vie privée du Canada (le « **Commissariat** ») a publié la version définitive de ses lignes directrices pour l'obtention d'un consentement valable, et donné des indications sur certaines « zones interdites » en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDE »**).

La LPRPDE prévoit que toute personne doit être « informée » de toute collecte, utilisation ou communication (collectivement, le « **Traitement** ») de renseignements personnels qui la concernent et y « consentir »[1], et que ce « consentement n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti »[2]. Les « **Lignes directrices pour l'obtention d'un consentement valable** », que le Commissariat a produites conjointement avec les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, énoncent les mesures que les organisations doivent ou devraient prendre pour s'assurer d'obtenir un consentement « valable ».

De plus, le paragraphe 5(3) de la LPRPDE prévoit qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[3].

Cette exigence quant au point de vue d'une personne raisonnable est distincte des exigences en matière de consentement prévues par la LPRPDE. Par conséquent, une organisation pourrait se trouver à contrevenir à la LPRPDE même si elle obtient un consentement au Traitement déraisonnable de renseignements personnels. Dans son « **Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)** », le Commissariat définit cinq « zones interdites » qui, selon lui, contreviennent à la LPRPDE du point de vue d'une personne raisonnable.

Dans le texte ci-dessous, nous examinons en profondeur deux nouveaux documents d'orientation du Commissariat, ainsi que les principales mesures que les organisations devraient prendre afin d'éviter toute

action coercitive.

Lignes directrices pour l'obtention d'un consentement valable – *Appliquées par le Commissariat à compter du 1er janvier 2019*

Le Commissariat a exprimé à plusieurs occasions des préoccupations concernant le fait que les organisations utilisent de longs énoncés légalistes des politiques de confidentialité comme fondement du Traitement de renseignements personnels. Les *Lignes directrices pour l'obtention d'un consentement valable* (les « **Lignes directrices sur le consentement** ») visent à « donner un nouveau souffle » aux différentes manières dont le consentement est obtenu, en énonçant sept principes directeurs. Le Commissariat s'attend à ce que les organisations suivent ces principes directeurs.

Dans l'ensemble, ces principes visent à offrir aux entreprises la marge de manœuvre nécessaire pour leur permettre d'élaborer leurs propres processus d'obtention de consentement, pourvu qu'elles créent des avis et des politiques sur la protection de la vie privée simples et lisibles que leurs consommateurs peuvent comprendre.

Les sept principes directeurs sont les suivants :[4]

1. Mettre l'accent sur les éléments clés

L'information fournie sur le Traitement des renseignements personnels doit être facilement accessible dans son intégralité, mais les organisations devraient également éviter la surabondance d'information. Par conséquent, les individus doivent pouvoir examiner rapidement les éléments clés qui auront une incidence sur leur décision en matière de protection des renseignements personnels au départ, dont les éléments clés suivants :

i. Les renseignements personnels qui sont recueillis. L'information à ce sujet doit être « suffisamment précise ».
ii. Les tiers auxquels les renseignements personnels sont communiqués, y compris le type de renseignements communiqués. Plus particulièrement, les organisations devraient expliquer toute communication à des tiers susceptibles d'utiliser les renseignements à leurs propres fins.
iii. Les fins du Traitement de données. Les personnes devraient avoir « suffisamment de détails » sur ces fins, et une distinction devrait être établie entre les fins qui sont essentielles à la prestation d'un service et celles qui ne le sont pas.
iv. Tout risque de préjudice et autres conséquences pour la personne. Ceci comprend seulement les « risques importants » de préjudice grave, à savoir les risques résiduels qui se situent en deçà de la prépondérance des probabilités (mais qui sont supérieurs à une simple possibilité) après que

> l'organisation a appliqué des mesures d'atténuation raisonnables. Par « préjudice grave » on entend notamment « la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles, la perte financière et le vol d'identité, l'effet négatif sur le dossier de crédit et le dommage aux biens ou leur perte ».

Le Commissariat a indiqué que les organisations devaient accorder une importance accrue aux quatre éléments mentionnés ci-dessus pour satisfaire aux exigences relatives à l'obtention du consentement prévues par la LPRPDE.

2. Permettre aux individus de déterminer à quel point et quand ils souhaitent obtenir de l'information détaillée

La quantité d'information dont une personne a besoin pour prendre une décision en matière de consentement varie selon la personne L'information sur la protection des renseignements personnels devrait être présentée par couches afin que les consommateurs puissent l'examiner rapidement, mais également obtenir plus d'information s'ils le souhaitent. De plus, les individus devraient avoir accès à l'information pendant toute la durée de leur relation avec l'organisation, et ils devraient pouvoir en tout temps décider s'ils veulent maintenir leur consentement ou le retirer.

3. Donner clairement aux individus la possibilité de choisir « oui » ou « non »

On ne peut pas exiger des individus qu'ils fournissent des renseignements personnels au-delà de ce qui est nécessaire pour fournir le produit ou le service. Si la communication des renseignements personnels n'est pas essentielle, les individus doivent pouvoir facilement choisir de ne pas consentir.

Si le Traitement des renseignements personnels est essentiel à la fourniture du produit ou à la prestation du service, l'organisation doit expliquer pourquoi c'est le cas.

4. Faire preuve d'innovation et de créativité

Les organisations devraient tirer profit des capacités numériques et créer des processus de consentement dynamiques et conviviaux qui sont appropriés à l'interface de l'utilisateur. Les organisations pourraient penser à utiliser les avis « juste-à-temps », les outils interactifs (p. ex. les vidéos, les outils infographiques), et les interfaces mobiles personnalisées.

5. Prendre en compte la perspective du consommateur

Les processus de consentement doivent être conviviaux et être compréhensibles du point de vue du public cible visé par l'organisation. Les organisations pourraient envisager à ces fins les mesures suivantes : consulter les utilisateurs et obtenir leur point de vue, mettre les processus de consentement à l'essai, consulter des

spécialistes de la protection privée ou des organismes de réglementation, et/ou suivre une pratique exemplaire bien établie.

6. *Faire du consentement un processus dynamique et continu*

L'obtention du consentement devrait être un processus qui se poursuit à mesure que les organisations innovent, prennent de l'essor et évoluent. Les organisations doivent obtenir le consentement des utilisateurs avant d'apporter des modifications significatives à leur politique de protection de la vie privée (p. ex., l'utilisation de renseignements personnels à des fins nouvelles non prévues à l'origine, ou la nouvelle communication de renseignements personnels à d'autres fins que le Traitement). Les organisations devraient répondre aux questions portant sur la protection de la vie privée au moyen de foires aux questions, d'assistants virtuels et autres technologies.

7. *Être responsable : se tenir prêt à démontrer en tout temps sa conformité*

Les organisations devraient être en mesure de démontrer que leur processus de consentement est compréhensible du point de vue du public cible. Il ne suffit pas de signaler quelques mots « dissimulés » dans une politique de confidentialité.

En plus de ces sept « principes directeurs », les Lignes directrices sur le consentement décrivent certains autres éléments applicables à l'obtention d'un consentement valable, dont les éléments suivants :

- Pour déterminer la forme de consentement appropriée, les organisations doivent prendre en compte le caractère sensible des renseignements et les attentes raisonnables de la personne.
- Les organisations doivent généralement obtenir un consentement explicite si les renseignements sont sensibles, ou en cas de Traitement des renseignements auquel la personne ne s'attendrait pas raisonnablement ou créant un risque résiduel important de préjudice grave.
- Dans le cas des enfants de moins de 13 ans, le consentement doit être obtenu auprès d'un parent ou d'un tuteur dans la plupart des circonstances[5].
- Même si elles obtiennent le consentement de la personne, les organisations ne peuvent Traiter les renseignements à des fins qu'une personne raisonnable estimerait inacceptables.
- Si l'individu retire son consentement, l'organisation doit mettre fin à la collecte des données et devrait, autant que possible, supprimer, les renseignements personnels existants.
- « Le consentement n'est pas une solution miracle ». La LPRPDE prévoit d'autres obligations, telles que celles qui sont liées à la responsabilité générale, aux limites de la collecte, à l'exactitude et aux mesures de sécurité.

Enfin, en réponse aux commentaires qu'il a reçus des intéressés sur le projet de lignes directrices pour

l'obtention d'un consentement valable qui a été publié l'an dernier, le Commissariat a fourni une « liste de contrôle » des choses que les organisations « doivent faire » et de celles qu'elles « devraient faire » pour se conformer à la LPRPDE. Dans cette liste de contrôle, le Commissariat indique pour chacun des points susmentionnés s'il considère qu'il constitue une obligation découlant d'exigences juridiques, ou plutôt une recommandation de meilleures pratiques.

Principales mesures pour les organisations

Le Commissariat a indiqué que la raison pour laquelle il a prévu que les Lignes directrices sur le consentement s'appliqueront à compter du 1er janvier 2019, est qu'il comprend que les organisations devront modifier leurs processus de consentement pour se conformer. Or, comme toute organisation qui a pris récemment une initiative en vue de se conformer au Règlement général sur la protection des données (RGPD) le sait, la modification de politiques et de pratiques en matière de protection de la vie privée prendra du temps. Par conséquent, les organisations devraient entreprendre dès maintenant l'examen des Lignes directrices sur le consentement (en particulier la « liste de contrôle »), et examiner leurs processus de consentement actuels afin d'établir et de mettre en œuvre toutes les modifications nécessaires.

Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3) – *Sera appliqué par le Commissariat à compter du 1er juillet 2018.*

Le paragraphe 5(3) de la LPRPDE se lit comme suit : « L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Par conséquent, même si la personne a donné son consentement, ses renseignements personnels ne peuvent être Traités qu'à des fins acceptables. De l'avis du Commissariat, ce paragraphe de la LPRPDE établit une distinction entre les formes légitimes de gestion des renseignements et les « zones interdites » illégitimes. Dans son Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3) (le « **Document d'orientation sur les pratiques inacceptables** »), le Commissariat énonce, à la lumière des décisions judiciaires antérieures, son interprétation du paragraphe 5(3) et définit les zones interdites qui devraient généralement être considérées comme contrevenant à la LPRPDE.

Dans l'ensemble, selon le Document d'orientation sur les pratiques inacceptables, le principe directeur qui sous-tend l'application du paragraphe 5(3) est que l'on doit parvenir à un équilibre entre le droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et le besoin de l'organisation de les Traiter.

À l'instar des Lignes directrices sur le consentement, le Document d'orientation sur les pratiques inacceptables mentionne clairement que les organisations doivent montrer que le Traitement des renseignements

personnels est raisonnable dans les circonstances, même si les individus ont consenti à un tel Traitement.

Pour déterminer si les fins du Traitement des renseignements personnels sont acceptables dans les circonstances, les tribunaux vont prendre en compte les faits particuliers dans les circonstances, dont les suivants :

- le caractère sensible des renseignements personnels;
- le besoin commercial légitime de la collecte des renseignements;
- l'efficacité du Traitement des renseignements pour répondre à ce besoin commercial;
- l'existence de moyens portant moins atteinte à la vie privée qui permettent d'atteindre les mêmes fins;
- la proportionnalité de l'atteinte à la vie privée par rapport aux avantages[6].

En se fondant sur ce qui précède, le Commissariat définit dans son Document d'orientation sur les pratiques inacceptables six pratiques qu'il considère actuellement comme des « zones interdites » en vertu de la LPRPDE.

1. Collecte, utilisation ou communication qui autrement est illégale

Les organisations devraient connaître les lois fédérales et provinciales du Canada et ne devraient pas Traiter des renseignements personnels d'une manière qui contrevient à ces lois. Par exemple, les organisations ne peuvent Traiter des renseignements personnels d'une manière qui contrevient aux lois régissant les rapports de solvabilité; elles ne peuvent non plus obliger les individus à subir un test génétique ou à en communiquer les résultats.

2. Profilage ou catégorisation donnant lieu à un traitement injuste, contraire à l'éthique ou discriminatoire interdit en vertu de la législation sur les droits de la personne

Une analyse des données, ou tout autre type de profilage ou de catégorisation, qui entraîne une discrimination fondée sur les motifs interdits en vertu de la législation sur les droits de la personne sera généralement jugé inacceptable en vertu de la LPRPDE. Le profilage ou la catégorisation injuste ou contraire à l'éthique qui ne contrevient pas à la législation sur les droits de la personne pourrait également être jugé inacceptable, et devra être évalué au cas par cas.

3. Collecte, utilisation ou communication à des fins qui causent ou sont susceptibles de causer un préjudice probable et grave à des individus

La collecte de données n'est pas acceptable si celle-ci cause ou est susceptible de causer un préjudice grave à des individus, notamment une lésion corporelle, une humiliation, des dommages à la réputation ou aux relations, une perte d'emploi ou d'occasions d'affaires ou d'activités professionnelles, une perte financière, un

vol d'identité, et/ou des dommages aux biens ou la perte de ceux-ci.

4. Publication de renseignements personnels dans le but de réclamer un paiement aux individus pour retirer ces renseignements

Les organisations ne peuvent publier en ligne des renseignements personnels principalement dans le but de réclamer un paiement aux individus pour retirer ces renseignements. Cela équivaut à du chantage, et a déjà été considéré comme contrevenant à la LPRPDE.[7]

5. Obligation de communiquer le mot de passe des comptes de médias sociaux aux fins de la sélection des employés

Les employeurs ne peuvent obliger des candidats à un poste ou des employés à leur communiquer leurs mots de passe des comptes de médias sociaux aux fins de l'obtention d'un emploi ou du maintien de leur emploi.

6. Surveillance exercée par une organisation au moyen des fonctions audio ou vidéo de l'appareil de l'individu lui-même

Même avec le consentement de l'individu, les organisations ne peuvent recueillir des renseignements sous format audio, texte ou vidéo au moyen du téléphone ou de l'ordinateur de l'individu. Toutefois, l'activation régulière ou constante des fonctions audio ou vidéo d'un appareil pour fournir un service peut être autorisée si l'individu est pleinement conscient de cette pratique et exerce un contrôle sur celle-ci et que les renseignements ne sont pas enregistrés, utilisés, communiqués ni conservés dans un but autre que celui de fournir le service en question.

Principales mesures pour les organisations

Le Commissariat n'a prévu qu'une courte période de transition avant la mise en application du Document d'orientation sur les pratiques inacceptables étant donné que ces pratiques interdites sont conformes aux interprétations antérieures de la LPRPDE. Par conséquent, les organisations devraient évaluer leurs pratiques actuelles de gestion des renseignements avant le 1er juillet afin de s'assurer que leur Traitement des renseignements personnels n'entre pas dans l'une des zones interdites définies par le Commissariat.

par Lyndsay Wasser et Sarah Strban (étudiante en droit)

[1] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, annexe 1, art. 4.3 [*LPRPDE*].
[2] *Ibid* à l'art. 6.1.
[3] *Ibid* au paragr. 5(3).
[4] Voir.

[5] Les organismes de réglementation de l'Alberta, de la Colombie-Britannique et du Québec n'étaient pas d'accord avec le fait qu'il convenait de fixer un âge minimum.
[6] *Turner* c. *Telus Communications Inc,* 2005 CF 1601 au paragr. 48, 144 ACWS (3d) 392.
[7] *A.T.* c. *Globe24h.com*, 2017 CF 114 aux paragr. 78-79, 275 ACWS (3d) 155.

Mise en garde