LANGLOIS

AVOCATS - LAWYERS

Le RGPD et le régime canadien de protection des renseignements personnels : quelles sont les différences?

Depuis son entrée en application le 25 mai dernier, le Règlement général sur la protection des données (RGPD) de l'Union européenne est devenu l'un des principaux points de référence en matière de protection de la vie privée et de confiance numérique à travers le monde.

S'il est vrai qu'une décision d'adéquation de la Commission européenne reconnaît qu'au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) assure un niveau de protection « adéquat » à l'égard des données à caractère personnel, cette décision a été rendue sous la Directive 95/46/CE sur la protection des données personnelles, laquelle a été remplacée par le RGPD.

Il existe désormais des différences significatives entre les deux régimes de protection de la vie privée. Partant, les organisations canadiennes assujetties au RGPD ne peuvent présumer de leur conformité du seul fait de leur respect des règles et des principes énoncés dans la LPRPDE. L'inverse est aussi vrai pour les entreprises de l'Union faisant ou souhaitant faire des affaires au Canada.

Le présent article se veut un portrait sommaire et pratique de certaines des plus importantes différences entre les deux régimes.[1]

Portée d'application

Le RGPD s'applique non seulement au traitement de données à caractère personnel par des organisations qui ont un établissement dans l'Union (indépendamment du lieu où sont traitées ces données), mais également au traitement par toute organisation à l'extérieur de l'Union relativement à une offre de biens ou de services à des personnes situées sur le territoire de l'Union ou au suivi de leur comportement au sein de l'Union.[2] Ainsi, une entreprise canadienne n'ayant aucun établissement dans l'Union peut être assujettie au RGPD dans la mesure où le traitement effectué rencontre les critères pour son application extraterritoriale.

La LPRPDE s'applique de manière générale aux renseignements personnels détenus par les organisations du secteur privé qui exercent leurs activités au Canada, sauf en Alberta, en Colombie-Britannique et au Québec (ces trois provinces ont des lois qui sont essentiellement similaires à la LPRPDE). La LPRPDE s'applique également aux transferts interprovinciaux ou internationaux de renseignements personnels.[3] Ainsi, une entreprise établie dans l'Union, mais exerçant une activité commerciale « réelle et importante » au Canada, se devra d'observer le droit canadien.

« …les entreprises n'ont pas à obtenir le consentement si elles peuvent démontrer que le traitement est nécessaire aux fins de la poursuite d'intérêts légitimes par le responsable du traitement ou par un tiers… »

Une des innovations du RGPD, qui n'a pas d'équivalent à l'heure actuelle au Canada, est cependant le fait que les sous-traitants se voient imposer des obligations spécifiques et encourent une mise en cause directe de leur responsabilité en cas de manquement au RGPD. Ainsi, au-delà des cas d'application directe, toute entreprise canadienne qui dessert des clients qui sont assujettis ou qui desservent eux-mêmes des entreprises assujetties en lien avec des activités au sein de l'Union, doit dès maintenant anticiper l'ajout d'exigences de conformité au RGPD comme condition contractuelle.

Fondements légaux du traitement

En vertu du RGPD, le consentement ne constitue qu'un fondement légal parmi d'autres pour justifier le traitement de données à caractère personnel. Entre autres, les entreprises n'ont pas à obtenir le consentement si elles peuvent démontrer que le traitement est nécessaire aux fins de la poursuite d'intérêts légitimes par le responsable du traitement ou par un tiers (à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée).

Au Canada, le consentement est la pierre angulaire du régime de protection des données à caractère personnel (appelées « renseignements personnels »). Sans consentement, une organisation assujettie à la LPRPDE ne peut traiter de renseignements personnels que dans certains cas d'exception bien précis. Toutefois, contrairement au RGPD qui requiert qu'un consentement soit explicitement donné pour être valide, il peut être implicite en droit canadien, c'est-à-dire raisonnablement déduit de l'action ou de l'inaction d'une personne en fonction du contexte et de la notion d'attentes raisonnables.

Droits des personnes concernées

Le RGPD octroie aux personnes concernées davantage de contrôle sur leurs données à caractère personnel. Au-delà des droits d'accès et de rectification, elles ont notamment le « droit à la portabilité des données » (c'est-à-dire le droit de recevoir, dans un format structuré, couramment utilisé et lisible par machine, les données à caractère personnel qui les concernent et qu'elles ont fournies). Le RGPD reconnaît également le « droit à l'effacement » (c'est-à-dire le droit d'obtenir, dans certaines circonstances, l'effacement de leurs données dans les meilleurs délais).

Ces droits n'ont pas d'équivalent dans la LPRPDE. Toutefois, le Commissariat à la protection de la vie privée du Canada s'est adressé à la Cour fédérale du Canada en octobre dernier pour obtenir des précisions sur la LPRPDE, afin de déterminer si un droit au « déréférencement » (soit la suppression de liens des résultats de recherche sans supprimer le contenu lui-même) existe au Canada.[4] Ce dossier, qui implique notamment Google, sera suivi de près.

Privacy by design

Le RGPD incorpore la notion de « protection de la vie privée dès la conception » (*privacy by design*, en anglais). Selon cette notion, les fabricants de produits, les prestataires de services et les producteurs d'applications doivent prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications.

Cette notion n'est pas reproduite dans la LPRPDE. On peut dire que cela est ironique puisque l'approche repose sur les principes développés au Canada dans les années 90 par D^re^ Ann Cavoukian, qui fut commissaire à l'information et la vie privée de l'Ontario.

Notifications d'incidents de sécurité

En vertu du RGPD, l'autorité de contrôle compétente doit être informée dans les meilleurs délais et, si possible, soixante-douze heures au plus tard après que le responsable du traitement ait pris connaissance d'une violation « susceptible d'engendrer un risque pour les droits et libertés de personnes physiques ». Les personnes concernées doivent aussi être informées dans les meilleurs délais, mais uniquement lorsque la violation est susceptible d'engendrer un « risque élevé » pour leurs droits et libertés, sauf si des mesures de protection appropriées ont été mises en place.

En vertu de la LPRPDE, le Commissariat à la vie privée du Canada et les « personnes intéressées » doivent être notifiées « le plus tôt possible » lorsqu'il est raisonnable de croire que la violation engendrera un « risque réel de préjudice grave » pour les personnes intéressées. La notion de préjudice grave est interprétée largement, comprenant un large éventail de situations telles que « la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la

perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles ».

En cas d'atteinte à des renseignements personnels, les entreprises doivent donc être conscientes que différents régimes de notification pourraient trouver application, chacun ayant ses particularités (délais applicables, types d'information à fournir, à qui, etc.).

Pouvoir d'exécution et sanctions

Le RGPD octroie de larges pouvoirs d'exécution aux autorités de contrôle, notamment par l'imposition d'amendes administratives, dont les pouvoirs suivants :

- conduire des enquêtes sous forme d'audit sur la protection des données;
- imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;
- ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;
- ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement;
- ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

Les contraventions au RGPD peuvent entraîner des amendes administratives coûteuses, lesquelles sont émises en fonction de la gravité de l'infraction, pouvant aller jusqu'à une amende de 20 000 000 d'euros (soit environ 30 000 000 $ CA) ou, si le résultat est plus élevé, 4 % du chiffre d'affaires annuel mondial dans le cas d'une entreprise qui commet une faute grave (par exemple, une violation des conditions applicables au consentement, violation des droits des personnes concernées, violation des transferts de données personnelles à un destinataire situé dans un pays tiers ou à une organisation internationale).

Le 21 janvier dernier, la Commission nationale de l'informatique et des libertés (CNIL) a d'ailleurs prononcé une sanction de 50 millions € contre Google pour violations continues du RGPD, notamment pour manque de transparence, information insatisfaisante et absence de consentement valable en lien avec la publicité personnalisée.[5]

« Les contraventions au RGPD peuvent entraîner des amendes administratives coûteuses… »

Sous le régime de la LPRPSP, le Commissaire à la vie privée du Canada n'a pas de pouvoirs aussi étendus. Certes, il a de vastes pouvoirs d'enquête, comme celui d'assigner à comparaître et d'exiger la présentation d'éléments de preuve. Il peut aussi, à toute heure raisonnable, pénétrer dans tout local occupé par une organisation. Mais, une fois l'enquête terminée, le Commissaire ne peut qu'émettre des recommandations non contraignantes à l'organisation ayant fait l'objet de l'enquête. Si cette dernière refuse ou néglige de les mettre en œuvre, le Commissaire doit alors se pourvoir devant la Cour fédérale et demander une ordonnance judiciaire pour faire appliquer ses recommandations.

Conclusion

De nos jours, les enjeux de protection des renseignements personnels et de cybersécurité plus généralement, dépassent l'aspect technologique. Ils affectent la façon même dont les entreprises se doivent d'opérer et de prendre des décisions d'affaires. Il est ainsi primordial, pour toute personne en affaires, d'être sensible aux diverses notions légales pouvant trouver application dans le marché global. De fait, de bonnes pratiques de conformité en pareilles matières représentent un avantage concurrentiel indéniable pour toute entreprise.

Consulter un conseiller juridique dans le cadre de cette démarche permettra de bien apprécier le champ d'application et les obligations imposées par les différents régimes juridiques applicables aux activités de votre organisation, d'éviter des erreurs potentiellement coûteuses et de répondre aux attentes de vos clients et partenaires d'affaires.

Auteurs

Caroline Deschênes, CIPP/C
Avocate, associée
T +1 438 844 7827
caroline.deschenes@langlois.ca

Pascal Archambault, CIPP/C
Avocat
T +1 514 282 7817
pascal.archambault@langlois.ca

Notes

1 Il existe d'autres différences et vous êtes invités à nous joindre pour toute question ou complément d'information.

2 La citoyenneté, la résidence ou tout autre statut juridique de la personne concernée n'a pas d'incidence dans ces situations. Par ailleurs, le traitement de données à caractère personnel de citoyens européens situés à l'extérieur de l'Union n'entraîne pas en soi l'application du RGPD. Pour plus de précisions, vous pouvez consulter les Lignes directrices sur le champ d'application territorial du RPDPD, publiées par le Conseil européen de la protection des données en novembre 2018 (en anglais seulement).

3 Elle s'applique aussi aux renseignements personnels concernant les employés d'entreprises sous réglementation fédérale canadienne (banques, entreprises de télécommunication, etc.), peu importe où elles se trouvent.

4 https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/an_181010/

5 https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la