Le Règlement général sur la protection des données (RGPD) : un fardeau ou une occasion?

6 novembre 2018

Auteurs

Sonia Rasquinha

Avocate

Roxane Fortin Lecompte

Étudiante

Gabriella Settino

La portée du nouveau Règlement

Les règles relatives à la protection des données à caractère personnel ont subi un changement fondamental avec l'entrée en vigueur du Règlement général sur la protection des données (RGPD) le 25 mai 2018. Cet ensemble de règles concernant la protection des données à caractère

personnel s'applique dans toute l'Union européenne (UE) et réglemente le traitement par une personne, une entreprise ou une organisation des données à caractère personnel concernant des personnes physiques au sein de l'Union européenne[1].

Le RGPD a pour objectif de redonner aux consommateurs le contrôle sur leurs données personnelles, et la portée du Règlement est vaste : toutes les sociétés exerçant des activités dans l'UE seront dorénavant assujetties à cet ensemble de règles unique, peu importe où elles sont établies et peu importe où le traitement de leurs données s'effectue[2]. De nombreuses entreprises canadiennes seront appelées à relever de nouveaux défis pour veiller à ce que leurs pratiques de collecte et de traitement des données soient conformes à ce nouveau régime de protection des données à caractère personnel.

Cela dit, une focalisation trop importante sur la conformité ou les sanctions est susceptible d'occulter les occasions potentielles qui pourraient découler de l'application du RGPD. En effet, l'entrée en vigueur de ce nouveau règlement représente une occasion pour les entreprises de maximiser leur valeur commerciale en fournissant aux consommateurs des lignes directrices claires et transparentes en ce qui a trait à l'utilisation, à la divulgation et à la conservation de leurs données à caractère personnel.

Quelles organisations canadiennes seront touchées par le RGPD?

Puisque le RGPD impose aux organisations des obligations plus coûteuses que les lois canadiennes sur la protection de la vie privée, il est impératif que les entreprises soient au fait de la vaste portée territoriale et matérielle de ce règlement.

Le RGPD s'applique aux entreprises canadiennes qui ont un établissement dans l'UE, indépendamment de l'endroit où les données à caractère personnel sont traitées, et aux entreprises canadiennes qui traitent des données pour :

> proposer des biens ou des services (payants ou gratuits) à des personnes qui résident dans l'UE;
> surveiller le comportement de personnes dans l'UE[3].

Il convient de noter que le Royaume-Uni sera assujetti au RGPD, malgré son intention de se retirer de l'UE le 29 mars 2019. Au cours de la période entre l'entrée en vigueur du RGPD et le retrait du Royaume-Uni de l'UE, le Royaume-Uni devra se conformer au RGPD en tant que membre de l'UE. En outre, les entreprises du Royaume-Uni qui continueront d'avoir des relations commerciales avec l'UE devront se conformer au RGPD afin d'éviter toute infraction[4].

En raison de la vaste portée du RGPD, les organisations canadiennes touchées par ce nouveau règlement devront s'assurer de respecter les nouvelles exigences qui y sont prévues. Le RGPD impose plusieurs obligations qui vont au-delà des exigences établies par la loi fédérale canadienne régissant la protection des renseignements personnels dans le secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). C'est notamment le cas des exigences relatives au consentement et de l'information qui doit être fournie aux personnes concernées.

Exigences relatives au consentement

La notion de consentement est un fondement juridique qui sous-tend à la fois la LPRPDE et le RGPD, mais ces deux documents législatifs adoptent des approches différentes à son égard en matière de traitement des données. Un consentement est considéré comme valable en vertu de la

LPRPDE « s'il est raisonnable de s'attendre à ce qu'un individu 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 »[5], et peut être *explicite* ou *implicite*, dans des circonstances bien définies et en fonction de la sensibilité des renseignements ou des attentes de la personne concernée.

Toutefois, en vertu du RGPD, le consentement est valide uniquement lorsqu'il est donné de façon libre, spécifique et univoque, par une déclaration ou un acte positif clair[6]. Le silence, l'inaction et les cases précochées ne constituent pas des actes positifs[7]. Les entreprises canadiennes assujetties au RGPD doivent revoir les méthodes qu'elles utilisent pour obtenir des consentements, en particulier dans les cas où un consentement implicite ou négatif suffisait précédemment. De plus, même si le consommateur y consent de façon explicite, le traitement de données sur l'origine raciale ou ethnique, sur les opinions politiques ou sur l'état de santé est interdit[8].

L'obtention d'un consentement conforme aux exigences du RGPD représente une bonne occasion pour les organisations d'accroître la confiance des personnes concernées à l'égard de leur stratégie de gouvernance des données. Dans le cadre du RGPD, le contrôleur doit fournir des renseignements précis aux consommateurs, soit : la période durant laquelle les données à caractère personnel seront conservées, ainsi qu'une description de tout traitement automatisé auquel les données seront soumises à des fins de prise de décisions ou de profilage.

Les organisations qui adoptent une approche transparente pour la gestion des violations de données à caractère personnel (lesquelles doivent être communiquées aux consommateurs lorsqu'elles sont susceptibles d'engendrer un risque élevé pour leurs droits et libertés[9]) sont plus susceptibles de gagner la confiance des consommateurs.

Qu'en est-il des lois provinciales sur la protection des renseignements personnels?

Le Québec, notamment, a sa propre loi en matière de protection des renseignements personnels (la *Loi sur la protection des renseignements personnels dans le secteur privé*), qui réglemente la collecte, l'utilisation et la communication des renseignements personnels dans la province. La LPRPDE s'applique tout de même au Québec pour ce qui est de la collecte, de l'utilisation ou de la communication de renseignements personnels en lien avec des entreprises fédérales[10].

La loi québécoise est considérée comme essentiellement similaire à la LPRPDE, c'est-à-dire qu'elle fournit un mécanisme de protection conforme et équivalent à celui de la LPRPDE et intègre les mêmes principes que la LPRPDE[11]. Par conséquent, le RGPD aura sensiblement les mêmes effets en matière de protection des renseignements personnels au Québec que dans les autres provinces canadiennes où seule la LPRPDE s'applique.

Quel rôle les cabinets d'avocats canadiens peuvent-ils jouer dans ce nouveau contexte réglementaire?

Le non-respect du RGPD peut donner lieu à des pénalités très sévères. Les contrevenants sont en effet passibles d'amendes pouvant atteindre le plus élevé des montants suivants :
20 000 000 d'euros ou 4 % de leur chiffre d'affaires mondial pour l'année précédente[12]. De plus, il est fort probable qu'une pénalité imposée en application du RGPD porte atteinte à l'image de l'entreprise concernée. En raison de ces risques financiers et d'atteinte à la réputation importants, les organisations canadiennes ont tout avantage à prendre au sérieux l'observation du RGPD. Il convient de noter qu'au mois de septembre de cette année, le Bureau du commissaire à

l'information du Royaume-Uni a engagé une première mesure formelle d'application du RGPD à l'endroit d'une entreprise d'analytique canadienne, AggregateIQ Data Services Ltd.

Les organisations qui se concentrent sur les effets positifs du RGPD peuvent en tirer des fruits allant bien au-delà de la simple conformité. À titre d'exemple, les consommateurs sont beaucoup plus susceptibles de faire confiance à un fournisseur de services qui accorde une grande importance au respect de la vie privée et qui fait preuve de transparence quant à la façon dont il utilise les données des personnes concernées.

---

1. Commission européenne, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_fr, art. 1 RGPD.
2. *Ibid*.
3. Art. 3 RGPD
4. « GDPR and Brexit », *GDPR Associates*, en ligne : <https://www.gdpr.associates/gdpr-brexit>.
5. Troisième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Consentement https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/principles/p_consentement/, LPRPDE, annexe 1, article 4.3.5
6. Par. 4(11) RGPD
7. Raison 32 RGPD
8. Art. 9 RGPD
9. Art. 34 RGPD
10. « Lois provinciales réputées essentiellement similaires à la LPRPDE », *Commissariat à la protection de la vie privée du Canada*, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/lois-provinciales-essentiellement-similaires-a-la-lprpde/> .
11. *Ibid*.
12. Art. 83.5 RGPD