EYB2022REP3468

Repères, Mai, 2022

Antoine AYLWIN* et Julie UZAN-NAULIN*

Chronique – Réforme de la protection des renseignements personnels (Loi 25) au Québec : le début d'un temps nouveau

Indexation

ACCÈS À L'INFORMATION ; PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ ; CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS ; DÉTENTION, UTILISATION ET NON-COMMUNICATION DES RENSEIGNEMENTS ; COMMUNICATION À DES TIERS ; APPLICATION ; DISPOSITIONS PÉNALES ; **COMMUNICATIONS ET TECHNOLOGIES**

TABLE DES MATIÈRES

Résumé

Les auteurs vous présentent la réforme de la protection des renseignements personnels au Québec issue de la Loi 25. Ce texte se concentre plus particulièrement sur les modifications apportées à la Loi sur la protection des renseignements personnels dans le secteur privé *en matière de responsabilisation des entreprises, de renforcement de la protection des renseignements personnels et de l'augmentation du montant des sanctions.*

INTRODUCTION

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (« Loi 25 ») a été adoptée le 21 septembre 2021 et sanctionnée le 22 septembre 2021.

Elle a pour objet de réformer les obligations incombant aux organismes publics et aux entreprises du secteur privé en matière de protection des renseignements personnels en modifiant la *Loi sur la protection des renseignements personnels dans le secteur privé*[1] (« Loi sur le secteur privé ») ainsi que la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[2]. Il est, en conséquence, important de prêter une attention toute particulière à cette nouvelle législation, qui impose notamment de nouvelles obligations aux entreprises québécoises tout en augmentant significativement les pouvoirs de la Commission d'accès à l'information.

Le présent article s'attache à décrire les nouvelles exigences introduites par la Loi 25 dans le secteur privé, s'inspirant en cela, dans une large mesure, du *Règlement général sur la protection des données* (« RGPD »)[3]. Ces nouvelles exigences, qui entrent en vigueur en trois étapes, peuvent être regroupées en deux grands axes : responsabilisation des entreprises et renforcement de la protection des renseignements personnels. En plus de ces changements, des sanctions élevées sont désormais prévues.

I– PREMIER AXE : RESPONSABILISATION DES ENTREPRISES

La Loi 25 entend responsabiliser les entreprises dans la gestion des renseignements personnels qu'elles collectent, utilisent ou communiquent. Cette responsabilisation prend différentes formes, mais des assouplissements sont également à relever.

A. Les différentes formes de responsabilisation : quelques exemples

1. La désignation d'une personne responsable de la protection des renseignements personnels

Jusqu'à présent, contrairement à ce qui est actuellement prévu par la loi fédérale, la *Loi sur la protection des renseignements personnels et les documents électroniques*[4] (« LPRPDÉ »), la Loi sur le secteur privé ne prévoit pas d'obligation de nommer une personne responsable de la protection des renseignements personnels.

Dans ce contexte, la Loi 25 vient combler cette lacune en prévoyant un nouvel article 3.1 à la Loi sur le secteur privé, qui prévoit la responsabilité de l'entreprise sur la protection des renseignements personnels qu'elle détient et la gestion de cette responsabilité par la nouvelle fonction de responsable de la protection des renseignements personnels.

Par défaut, la personne ayant la plus haute autorité au sein d'une entreprise du secteur privé devra exercer cette nouvelle fonction.

Cette fonction pourra être déléguée par écrit, en tout ou partie, à un membre du personnel. En outre, le titre et les coordonnées de cette personne responsable devront être rendus publics sur le site Internet de l'entreprise ou, si cette entreprise n'a pas de site, ces informations devront être rendues accessibles par tout autre moyen approprié.

Le responsable à la protection des renseignements personnels devra s'assurer que l'entreprise respecte les principes applicables, par exemple en établissant et mettant en oeuvre des politiques et pratiques encadrant la gouvernance de l'entreprise et la protection des renseignements personnels[5]. Le responsable devra également participer à l'évaluation des facteurs relatifs à la vie privée (« EFVP ») de tout projet de système d'information ou de prestation électronique[6] et être impliqué dans la gestion d'un incident de confidentialité[7].

Eu égard à l'importance de ses fonctions et aux sanctions pécuniaires[8] qui pourront être octroyées aux entreprises, le responsable devra avoir les compétences nécessaires pour être en mesure de mener correctement sa mission.

Cette nouvelle fonction, déléguée ou non, entrera en vigueur le 22 septembre 2022.

2. Une obligation de signalement des incidents de sécurité

À ce jour, la Loi sur le secteur privé ne prévoit aucune obligation de signalement d'incidents impliquant la fuite de renseignements personnels, ceci étant laissé à la discrétion des entreprises.

Cela va changer avec la Loi 25. En effet, le nouvel article 3.5 prévoit qu'à compter de septembre 2022, une entreprise doit aviser la Commission d'accès à l'information lorsqu'elle a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient, et que cet incident présente un risque qu'un préjudice sérieux soit causé.

Elle doit également aviser toute personne dont un renseignement personnel est concerné par l'incident ainsi que tout organisme susceptible de diminuer le risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.

À noter que, contrairement à ce qui existe en vertu du RGPD, aucun délai pour aviser ces parties n'est prévu, mais plutôt que le signalement doit se faire avec « diligence »[9].

L'incident de confidentialité est défini comme étant un accès, une utilisation ou une communication non autorisé par la loi à un renseignement personnel ou comme la perte d'un renseignement personnel, ou toute autre atteinte à la protection d'un tel renseignement[10]. Ainsi, cette définition est donc particulièrement large et englobe des situations aussi différentes que la perte d'une clef USB, des intrusions par un tiers dans le système informatique d'une organisation, l'attaque par rançongiciel, la perte de données provoquée par un virus ou par une faille informatique, l'extraction de données par un employé ou une personne non autorisée, etc.

Enfin, et comme au niveau fédéral avec la LPRPDÉ, la Loi 25 introduit l'obligation de tenir un registre des incidents de confidentialité, registre qui devra être transmis à la Commission à sa demande[11]. Un incident de confidentialité pourra ainsi laisser des taches persistantes sur l'image des organisations, alors que ce registre sera plus souvent demandé lors de vérifications diligentes préalables à la conclusion de partenariats, de toute autre transaction de nature commerciale ou même de litige mettant en cause la sécurité de l'information.

3. Mise en place de politiques et pratiques

La loi 25 oblige les entreprises à établir et mettre en oeuvre des pratiques en matière de protection des renseignements personnels[12] qui devront être approuvées par le responsable à la protection des renseignements personnels. Des informations détaillées au sujet de ces politiques et de ces pratiques devront être publiées sur le site Web de l'entreprise en termes simples et clairs, ce qui pourrait prendre la forme d'un espace « Vie privée » sur le site en question.

Ces politiques et pratiques devront notamment prévoir :

- les durées de conservation et destruction des renseignements personnels ;
- les rôles et responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements ; et
- un processus de traitement des plaintes.

Au sujet des durées de conservation, à ce jour, la Loi sur le secteur privé dispose que les renseignements personnels ne peuvent être conservés que pendant le temps nécessaire aux fins identifiées (Loi sur le secteur privé, art. 10) ou pour permettre à la personne concernée d'épuiser les recours prévus par la loi (Loi sur le secteur privé, art. 36) étant précisé que « l'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement » (Loi sur le secteur privé, art. 12), calendrier qui n'a jamais été établi.

La Loi 25 va plus loin au chapitre de la conservation des renseignements personnels : une fois que la finalité pour laquelle le renseignement personnel aura été accomplie, il sera obligatoire soit de détruire le renseignement en question, soit de l'anonymiser.

Si la notion de destruction ne pose pas de problème en soi, celle d'anonymisation peut être plus difficile à appréhender. C'est pourquoi le nouvel article 23 introduit par la Loi 25 en donne des critères :

- le procédé d'anonymisation doit être irréversible ;
- il doit être impossible d'identifier directement ou indirectement l'individu ;
- les renseignements anonymisés doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement.

Ainsi, ce faisant, la Loi 25 vient expliquer la distinction entre « anonymisation » et « dépersonnalisation ». Alors que l'anonymisation est un procédé qui ne permet plus d'identifier directement ou indirectement un individu, la dépersonnalisation (à laquelle réfère notamment le nouvel article 12) est un procédé qui ne permet plus d'identifier directement la personne concernée et qui permet, notamment, de conserver des renseignements lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques[13]. L'expression « indirectement » est donc au coeur de la distinction entre anonymisation et dépersonnalisation.

En tout état de cause, et comme l'affirme très clairement l'alinéa 3 du nouvel article 23, l'anonymisation devra être considérée comme une meilleure pratique.

Concrètement, cela signifie que les entreprises du secteur privé devront déterminer, dans des politiques accessibles au public, les durées de conservation dans les limites prévues par la loi ainsi que la façon dont les renseignements seront détruits, voire anonymisés ou dépersonnalisés. Cela devra être mis en place pour septembre 2023.

4. La mise en place d'études des facteurs relatifs à la vie privée

Avec l'adoption du RGPD, les analyses d'impact ne sont plus seulement une bonne pratique : elles sont maintenant une obligation dans bien des cas, notamment pour tout traitement de données effectué à l'aide de nouvelles technologies et « lorsque l'atteinte est susceptible d'engendrer un risque pour les droits et libertés » des personnes concernées[14]. Par conséquent, la responsabilité du respect de la vie privée ne repose plus uniquement sur les épaules des citoyens : elle incombe désormais à toutes les organisations.

Cette même approche est préconisée au Québec par la Loi 25, qui rend obligatoire les EFVP notamment pour « tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels » mis en place à compter de septembre 2023[15]. Cette doit se faire en fonction « de la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support ».

Cette disposition, qui a pourtant évolué dans le bon sens, demeure préoccupante. D'abord, il n'y a aucune raison que ce type d'évaluation soit réservée aux projets technologiques (et incidemment ayant une composante d'IA), ce qui va d'ailleurs à l'encontre du principe de neutralité technologique.

Ensuite, une telle disposition suggère que tout professionnel offrant un algorithme utilisant un ou plusieurs renseignements personnels devra systématiquement évaluer le type et le degré de détails afférents à l'EFVP, le critère de proportionnalité étant hautement subjectif et risquant de créer une certaine confusion.

Finalement, l'expérience de conformité RGPD démontre que l'EFVP est loin d'être un exercice sans conséquence : il requiert l'implication de nombreux intervenants, peut prendre plusieurs semaines à compléter, demeure tributaire de nombreuses ressources, et doit donc se limiter aux projets présentant des risques élevés pour les individus.

5. Des transferts encadrés

À compter de septembre 2023, tout transfert de renseignement personnel à l'extérieur du Québec devra reposer sur une EFVP qui devra tenir compte de plusieurs facteurs, tels que les mesures de protection, y compris celles qui sont contractuelles, dont le renseignement bénéficierait et le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables[16].

Cette évaluation devra démontrer « que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus ». Cette expression n'est pas définie et il est difficile de prévoir comment elle sera interprétée en pratique.

Ces modifications vont rendre plus difficiles les transferts hors Québec : le Québec sera, avec l'Union européenne, l'une des seules juridictions au monde à imposer une EFVP pour tout transfert extra-provincial de renseignements personnels au lieu de se limiter à des mesures de protection (y compris contractuelles).

B. Des assouplissements bienvenus

Des assouplissements bienvenus sont apportés par la Loi 25, notamment en matière de communication de renseignements personnels.

Par exemple, à partir de septembre 2022, lorsque la communication d'un renseignement personnel est nécessaire aux fins de la conclusion d'une transaction commerciale à laquelle elle entend être partie, une entreprise peut communiquer un tel renseignement, sans le consentement de la personne concernée, à l'autre partie à la transaction. La transaction a été définie largement pour y inclure :

- l'aliénation ou la location d'une entreprise ou de ses actifs, en tout ou en partie ;
- la modification de la structure juridique de l'entreprise ;
- l'obtention d'un prêt ou d'une autre forme de financement ;
- la prise d'une sûreté, afin de garantir une de ses obligations[17].

Il en va de même pour la possibilité de communiquer des renseignements personnels à une personne ou un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques, et ce, sans le consentement des personnes concernées. La Loi 25 met donc fin, dès septembre 2022, à la procédure d'autorisation auprès de la Commission d'accès à l'information en matière d'évaluation des demandes d'autorisation des communications à des fins de recherche et à son pouvoir de révocation.

Toutefois, des garde-fous sont mis en place, comme la nécessité de procéder à une EFVP et de conclure avec la personne ou l'organisme à qui elle les transmet une entente de confidentialité contenant les exigences prévues par la loi[18].

II– DEUXIÈME AXE : LE RENFORCEMENT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Corrélativement à la responsabilisation des entreprises, la protection des renseignements personnels des individus se voit renforcée. La plupart des modifications entreront en vigueur à compter de septembre 2023.

A. Une information renforcée pour un consentement éclairé

Selon la Loi sur le secteur privé actuelle, afin que le consentement soit éclairé, la personne concernée doit être informée (i) de l'objet du dossier ; (ii) de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise ; (iii) de l'endroit où sera détenu son dossier ; ainsi que (iv) des droits d'accès ou de rectification.

Si les conditions pour l'obtention d'un consentement valide changent peu finalement (le consentement doit toujours être manifeste, libre et éclairé et être donné à des fins spécifiques), la Loi 25 prévoit plus spécifiquement les points suivants[19] :

- les fins auxquelles ces renseignements sont recueillis ;
- les moyens par lesquels les renseignements sont recueillis ;
- les droits d'accès et de rectification prévus par la loi ;
- le droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis (il est à noter que ce droit qui existait déjà auparavant est désormais codifié) ;
- le cas échéant, le nom du tiers pour qui la collecte est faite (nouveau) ;
- le cas échéant, la possibilité que les renseignements soient communiqués à l'extérieur du Québec (nouveau).

Par ailleurs, sur « demande de sa part », la personne concernée doit également être informée des éléments suivants :

- des renseignements personnels recueillis auprès d'elle ;
- des catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise ;
- de la durée de conservation de ces renseignements ;
- ainsi que des coordonnées du responsable de la protection des renseignements personnels (à noter que cette précision peut paraître superflue dès lors que l'article 3.1 dispose expressément que les coordonnées du responsable doivent être publiées sur le site Internet de l'entreprise).

Cette façon de rédiger en deux temps (informations principales et informations supplémentaires) se rapproche de l'article 13 du RGPD.

B. Une protection de la vie privée « par défaut »

La Loi 25 prévoit qu'une entreprise qui offre un produit ou un service technologique doit s'assurer que les paramètres de confidentialité de ces produits ou services offerts au public assurent le plus haut niveau de confidentialité, par défaut[20]. Cette exigence ne s'applique toutefois pas aux témoins de connexions (« cookies »).

De plus, lorsque la collecte des renseignements est faite par une technologie possédant des fonctions d'identification, de localisation ou de profilage, la personne doit être informée de la façon de les activer. C'est le choix « opt-in », changement du « opt-out » dans la version initiale du projet de loi 64, où le paramétrage par défaut était l'activation de ces fonctions. Cette disposition risquera d'être difficile d'application en pratique[21].

C. De nouveaux droits pour les individus

La Loi 25 introduit de nouveaux droits pour les individus, tendant à se rapprocher de ceux prévus par le RGPD, notamment :

- *le droit à l'oubli* (ou droit à la désindexation). La Loi 25 permet à une personne d'exiger d'une organisation de cesser de publier des informations personnelles ou de désindexer un hyperlien donnant accès à ces informations lorsque leur diffusion porte gravement atteinte à la réputation ou à la vie privée de la personne, et lorsque ce préjudice l'emporte clairement sur l'intérêt du public à connaître ces informations[22]. Ce nouveau droit est similaire à celui prévu par l'article 17 du RGPD, expliqué par la jurisprudence européenne[23] ;
- *le droit à la portabilité des données,* c'est-à-dire le droit d'un individu de recevoir les informations personnelles qu'il a fournies à une organisation dans un format technologique structuré et couramment utilisé. À la demande de cette personne, ces informations doivent être transmises à toute autre personne ou organisation. Ce nouveau droit vise tous les renseignements personnels qu'une entreprise détient sur une personne, à l'exception des renseignements créés, dérivés, calculés ou inférés à partir des renseignements fournis par la personne concernée (ex. : profil d'un utilisateur), lesquels peuvent avoir une valeur commerciale pour les entreprises. Ce nouveau droit ne concerne donc que les renseignements personnels fournis par la personne concernée à l'entreprise. Précisons, par ailleurs, que les nouveaux systèmes d'information ou de prestation électronique de service devront permettre la portabilité[24]. Contrairement aux autres droits mentionnés, celui-ci n'entrera en vigueur qu'à compter de septembre 2024 ;
- *les décisions fondées sur un traitement automatisé.* Dans ce cas, la personne doit, en plus des éléments énoncés ci-dessus, être informée de l'existence d'une prise de décision fondée exclusivement sur un traitement automatisé de renseignements personnels, et l'entreprise doit en informer la personne concernée[25]. Toutefois, contrairement au RGPD, la Loi 25 n'accorde pas le droit de ne pas être soumis à une décision automatisée.

III– SANCTIONS IMPORTANTES

À compter de septembre 2023, une entreprise qui ne respecterait pas ses obligations pourra se voir sanctionnée financièrement. Les montants des sanctions s'alignent sur celles du RGPD.

Les entités du secteur privé seront soumises à des amendes pouvant aller jusqu'à 25 000 000 $, ou à un montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent, selon le montant le plus élevé[26]. Cela représente une augmentation considérable par rapport à la pénalité maximale actuelle de 50 000 $, et ferait de la Loi sur le secteur privé, la loi sur la protection de la vie privée la plus punitive au Canada (avec une amende potentielle dépassant celles prévues par la loi sur la concurrence, ou la loi anti-pourriel, CASL.

De plus, des sanctions administratives pécuniaires peuvent également être imposées pour certaines infractions à la suite d'un avis de non-conformité de la Commission d'accès à l'information (avec un maximum de 10 000 000 $ ou, si ce montant est plus élevé, un montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent[27].

Là encore, la similitude avec le système d'amendes du RGPD est évidente. En effet, il convient de rappeler que l'article 83 RGPD prévoit des amendes pouvant aller, en fonction du type de violations au RGPD, jusqu'à 20 000 000 € ou 4 % du chiffre d'affaires annuel mondial.

CONCLUSION

Ce panorama de la réforme issue de la Loi 25 montre une tendance certaine à s'aligner sur le RGPD, actuellement le plus haut standard en matière de protection des renseignements personnels.

La question se pose de savoir si les autres provinces canadiennes et le fédéral vont suivre cette tendance. Des projets de réforme sont à l'étude, notamment en Colombie-Britannique qui entend réformer sa loi sur la protection des renseignements personnels[28] ainsi qu'au fédéral, bien que le projet de loi C-11 ait, semble-t-il, été abandonné.

Une harmonisation des lois canadiennes relatives à la protection de la vie privée serait en effet bienvenue, de même qu'une harmonisation de ces lois avec le RGPD. Cela faciliterait les échanges interprovinciaux ainsi que les transferts de renseignements vers, ou depuis, le Canada, sans ce soucier de la législation applicable et sans plus de formalités.

Pour en savoir plus, Fasken a mis à votre disposition un centre de ressources sur la Loi 25 accessible à l'adresse suivante : <https://www.fasken.com/fr/knowledge/projet-de-loi-64/2020/06/accueil>.

---

* M^{e} Antoine Aylwin, CIPP/C, est associé chez Fasken Martineau DuMoulin S.E.N.C.R.L. Il concentre sa pratique en litige successoral, fiduciaire et administratif. M^{e} Julie Uzan-Naulin, membre des Barreaux de Paris et de Montréal, est avocate-conseil au sein du groupe Protection de l'information et de la vie privée du même cabinet et est spécialiste du RGPD, et plus

généralement de la protection des données personnelles au Canada.

1. RLRQ, c. P. 39-1.

2. RLRQ, c. A-2.1.

3. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE).

4. L.C. 2000, ch. 5.

5. Loi sur le secteur privé amendée par la Loi 25, art. 3.1.

6. *Ibid.,* art. 3.2.

7. *Ibid.*, art. 3.5.

8. Voir Titre III.

9. Loi sur le secteur privé amendée par la Loi 25, art. 3.5.

10. *Ibid.*, art. 3.6.

11. *Ibid.*, art. 3.8.

12. *Ibid.*, art. 3.2.

13. Loi sur le secteur privé amendée, art. 12.

14. RGPD, art. 35.

15. *Ibid.*, art. 3.3.

16. *Ibid.*, art. 17.

17. *Ibid.*, art. 18.4.

18. *Ibid.*, art. 21 à 21.0.2.

19. *Ibid.*, art. 8.

20. Loi sur le secteur privé amendée, art. 9.1.

21. *Ibid.*, art. 8.1.

22. *Ibid.*, art. 28.1.

23. CJUE, 13 mai 2014, C-131/12, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González. En ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62012CJ0131&from=FR ; CJUE, 24 septembre 2019, C-507/17, Google LLC c. Commission nationale de l'informatique et des libertés (CNIL). En ligne : https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=fr&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctru

24. Loi sur le secteur privé amendée, art. 27.

25. *Ibid.*, art. 12.1

26. *Ibid.*, art. 91.

27. *Ibid.*, art. 90.12.

28. Personal Information Protection Act, [SBC 2003] c. 63. En ligne : https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01 ; voir par exemple Modernizing British Columbia's Private Sector Privacy Law. En ligne : https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/2nd-session/pipa/report/SCPIPA-Report_2021-12-06.pdf.

Date de dépôt : 18 mai 2022