Modifications aux lois sur la protection des renseignements personnels : ce que les entreprises doivent savoir

4 octobre 2021

Auteurs

Raymond Doray

Associé, Avocat

Guillaume Laberge

Associé, Avocat

Le projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* a été adopté le 21 septembre 2021 par l'Assemblée nationale et modifie une vingtaine de lois ayant trait à la protection des renseignements personnels, notamment la *Loi sur l'accès aux documents des organismes publics* (« ***Loi sur l'accès*** »), la *Loi sur la protection des renseignements personnels dans le secteur privé* (« ***Loi sur le secteur privé*** ») et la *Loi sur le cadre juridique des technologies de l'information*.

Bien que les changements touchent à la fois les organismes publics et les entreprises privées, le présent bulletin vise plus particulièrement à faire un survol des nouvelles exigences pour les entreprises privées visées par la *Loi sur le secteur privé*.

Nous avons préparé une version amendée de la Loi sur le secteur privé afin de refléter les changements apportés par le projet de loi n 64.

Essentiellement, la loi modifiée tend à donner un meilleur contrôle aux individus sur leurs renseignements personnels, à favoriser la protection des renseignements personnels, à responsabiliser davantage les entreprises et à introduire de nouveaux mécanismes visant à assurer le respect des règles en matière de protection des renseignements personnels. Voici une synthèse des principales modifications adoptées par le législateur ainsi que les nouvelles exigences imposées aux entreprises dans ce domaine.

Il importe de mentionner que ce nouveau régime de protection des renseignements personnels entrera en vigueur, en grande partie, dans deux ans.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

1. Accroître le contrôle des individus sur leurs renseignements personnels et la transparence

La nouvelle loi instaure le droit des individus d'accéder aux renseignements les concernant recueillis par les entreprises dans un format technologique structuré et couramment utilisé et d'en exiger la communication à un tiers, à l'exception des renseignements qui sont créés, dérivés, calculés ou inférés à partir des renseignements fournis par la personne concernée (art. 27). Ce droit est usuellement appelé « droit à la portabilité ».

Les entreprises ont maintenant une obligation de détruire les renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis ou utilisés sont accomplies. Les entreprises ont également la possibilité d'anonymiser les renseignements personnels selon les meilleures pratiques généralement reconnues pour les utiliser à des fins sérieuses et légitimes (art. 23). Toutefois, il importe que l'identité des individus concernés ne puisse être restaurée.

De plus, les entreprises privées doivent désindexer tout hyperlien permettant d'accéder aux renseignements personnels d'un individu (souvent appelé le droit au « déréférencement ») lorsque sa diffusion contrevient à la loi ou à une ordonnance judiciaire (art. 28.1).

Si une organisation prend une décision qui est fondée exclusivement sur le traitement automatisé de renseignements personnels, l'individu concerné doit en être informé, et à sa demande, si la décision produit des effets juridiques ou l'affecte autrement, il doit être informé des renseignements personnels qui ont été utilisés dans la prise de décision, ainsi que des raisons et des principaux facteurs ayant mené à celle-ci. La personne doit également être informée de son droit à la rectification (art. 12.1).

Les organisations qui ont recours à des moyens technologiques permettant d'identifier un individu, de le localiser ou d'effectuer son profilage doivent l'informer du recours à cette technologie et des moyens offerts pour désactiver ces fonctions (art. 8.1).

La communication et l'utilisation de listes nominatives par une entreprise privée à des fins de prospection commerciale ou philanthropique sont dorénavant assujetties au consentement de la personne concernée.

Les entreprises doivent maintenant publier sur leur site Internet en termes simples et clairs leurs règles de gouvernance à l'égard des renseignements personnels (art. 3.2). Ces règles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les diverses responsabilités des membres du personnel à l'égard des renseignements personnels. De plus, les entreprises qui recueillent des renseignements personnels par un moyen technologique devront également adopter et publier sur leur site Internet une politique de confidentialité en termes simples et clairs (art. 8.2).

La nouvelle loi prévoit également que les entreprises qui refusent une demande d'accès à l'information doivent dorénavant, en plus de motiver leur refus et d'indiquer la disposition de la *Loi sur le secteur privé* sur laquelle le refus s'appuie, prêter assistance au requérant qui le demande pour l'aider à comprendre ce refus (art. 34).

2. Favoriser la protection des renseignements personnels et la responsabilisation des entreprises

Le projet de loi n° 64 vise à accorder une plus grande part de responsabilité aux entreprises en matière de protection des renseignements personnels. C'est ainsi que les entreprises se voient imposer l'obligation de nommer un responsable de la protection des renseignements personnels, qui par défaut sera la personne ayant la plus haute autorité au sein de leur organisation (art. 3.1).

En outre, les entreprises devront réaliser une évaluation des facteurs relatifs à la vie privée (« **EFVP** ») pour tout projet d'acquisition, de développement et de refonte d'un système

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels (art. 3.3). Cette obligation force ainsi les entreprises à s'interroger dès le début d'un projet sur les risques que celui-ci soulève quant à la protection de la vie privée et des renseignements personnels. L'EFVP devra être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support (art. 3.3).

Les entreprises devront également procéder à une EFVP lorsqu'elles auront l'intention de communiquer des renseignements personnels à l'extérieur du Québec, afin de déterminer si les renseignements bénéficieront d'une protection adéquate eu regard notamment aux principes de protection des renseignements personnels généralement reconnus (art. 17). La communication devra aussi faire l'objet d'une entente écrite qui tient compte notamment des résultats de l'EFVP et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés (art. 17 (2)).

La communication par les entreprises des renseignements personnels à des fins d'études, de recherche ou de production de statistiques est aussi assujettie à la réalisation d'une EFVP (art. 21). De plus, ce régime est substantiellement modifié puisque le tiers qui souhaite utiliser les renseignements personnels à ces fins doit présenter une demande écrite à la Commission d'accès à l'information (« CAI »), joindre une présentation détaillée de ses activités de recherche et divulguer la liste de toutes les personnes et de tous les organismes auprès desquels il a fait une demande de communication similaire (art. 21.01.1 et 21.01.02).

Les entreprises peuvent aussi communiquer un renseignement personnel à un tiers, sans le consentement de l'individu concerné, dans le cadre de l'exécution d'un contrat de service ou d'entreprise. Le mandat devra faire l'objet d'un contrat écrit, qui devra notamment prévoir les mesures de protection des renseignements personnels à respecter par le mandataire ou le prestataire de service (art. 18.3).

La communication de renseignements personnels, sans le consentement des individus visés, dans le cadre d'une transaction commerciale entre entreprises privées fait l'objet d'un encadrement supplémentaire (art. 18.4). La notion de transaction commerciale s'entend de « l'aliénation ou de la location de tout ou partie d'une entreprise ou des actifs dont elle dispose, d'une modification de sa structure juridique par fusion ou autrement, de l'obtention d'un prêt ou de toute autre forme de financement par celle-ci ou d'une sûreté prise pour garantir une de ses obligations » (art. 18.4).

Les entreprises doivent détruire ou rendre anonymes les renseignements personnels recueillis lorsque les fins de la collecte ont été accomplies, sous réserve des délais de conservation prévus par une loi (art. 23). Il s'agit d'un changement important pour les entreprises privées qui peuvent présentement conserver des renseignements personnels caducs s'ils ne les utilisent pas.

La nouvelle loi impose aussi l'intégration du principe de la protection de la vie privée par défaut (*privacy by default*), ce qui implique que les entreprises qui recueillent des renseignements personnels en offrant au public un produit ou un service technologique disposant de divers paramètres de confidentialité doivent s'assurer que ces paramètres assurent par défaut le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée (art. 9.1). Cela ne s'applique pas aux paramètres de confidentialité d'un témoin de connexion (aussi appelés *cookies*).

Lorsqu'une entreprise a des motifs de croire qu'un incident de confidentialité est survenu, elle doit prendre des mesures raisonnables afin de réduire les risques de préjudice et les risques de récidives (art. 3.5). La notion d'incident de confidentialité est définie comme étant l'accès à un renseignement personnel ou l'utilisation, la communication ou la perte de renseignements personnels (art. 3.6). De plus, les entreprises ont l'obligation d'aviser les personnes concernées, ainsi que la Commission d'accès à l'information de chaque incident qui présente un risque sérieux de préjudice, qui s'évalue à la lumière de la sensibilité des renseignements concernés, des

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

conséquences appréhendées de leur utilisation et de la probabilité qu'ils soient utilisés à des fins préjudiciables (art. art. 3.7). Les entreprises devront également tenir un registre des incidents de confidentialité qui devra être communiqué à la CAI sur demande (art. 3.8).

3. Renforcer le régime d'obtention du consentement

La nouvelle loi modifie la *Loi sur le secteur privé* de façon à ce que le l'obtention de tout consentement qui y est prévu soit manifeste, libre et éclairé et qu'il soit donné à des fins spécifiques. Ce consentement doit de plus être demandé pour chacune des fins de la collecte, en termes simples et clairs et de manière distincte, de façon à éviter qu'il ne soit obtenu par le biais de conditions d'utilisation complexes et difficilement compréhensibles pour les personnes concernées (art. 14).

Le consentement des mineurs de moins de 14 ans à la collecte de renseignements personnels par les entreprises doit être donné par le titulaire de l'autorité parentale, alors que celui du mineur de 14 ans et plus pourra être donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur (art. 14).

Au sein d'une entreprise, le consentement à la communication d'un renseignement personnel sensible (par exemple des renseignements de santé ou par ailleurs intimes) doit être manifesté de façon expresse (art. 12).

4. Assurer une meilleure conformité aux exigences prévues à la *Loi sur le secteur privé*

La *Loi sur le secteur privé* est aussi modifiée par l'ajout de nouveaux mécanismes visant à faire en sorte que les entreprises assujetties respectent les exigences qui y sont prévues.

D'une part, la CAI se voit accorder le pouvoir d'imposer des sanctions administratives pécuniaires dissuasives aux contrevenants. Ces sanctions peuvent s'élever jusqu'à 10 000 000 $ ou 2 % du chiffre d'affaires mondial de l'entreprise (art. 90.12). En cas de récidive, ces amendes seront portées au double (art. 92.1).

De plus, lorsqu'un incident de confidentialité survient au sein d'une entreprise, la CAI peut lui ordonner de prendre des mesures visant à protéger les droits des individus concernés, après lui avoir permis de présenter des observations (art. 81.3).

Ensuite, de nouvelles infractions pénales sont créées, pouvant elles aussi mener à l'imposition d'amendes sévères. Pour les entreprises contrevenantes, ces amendes peuvent s'élever jusqu'à 25 000 000 $ ou 4 % de leur chiffre d'affaires mondial (art. 91).

Finalement, la nouvelle loi crée également un nouveau droit d'action privé. Essentiellement, celui-ci prévoit que lorsqu'une atteinte illicite à un droit conféré par la *Loi sur le secteur privé* ou par les articles 35 à 40 du *Code civil* cause un préjudice et que cette atteinte est intentionnelle ou résulte d'une faute lourde, les tribunaux peuvent accorder des dommages-intérêts punitifs d'une valeur minimale de 1000 $ (art. 93.1).

5. Entrée en vigueur

Les modifications apportées par le projet de loi n° 64 entreront en vigueur en plusieurs étapes. La majorité des nouvelles dispositions de la *Loi sur le secteur privé* entreront en vigueur deux ans suivant la date de la sanction de la loi, qui était le 22 septembre 2021. Certaines dispositions spécifiques entreront toutefois en vigueur un an après cette date, dont notamment :

L'obligation pour les entreprises de désigner un responsable de la protection des renseignements personnels (art. 3.1)
L'obligation de signalement des incidents de confidentialité (art. 3.5 à 3.8)
L'exception à la communication de renseignements personnels dans le cadre d'une transaction commerciale (art.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

18.4) et
L’exception à la communication de renseignements personnels pour des fins d’études ou de recherche (art. 21 à 21.0.2).

D’autre part, la disposition consacrant le droit à la portabilité des renseignements personnels (art. 27) entrera en vigueur trois ans suivant la sanction de la loi.

Les membres de l’équipe Lavery sont disponibles pour répondre à vos questions et pour vous aider à vous conformer aux nouvelles exigences en matière de protection des renseignements personnels introduites dans la *Loi sur le secteur privé*.

Les informations et commentaires contenus dans le présent document ne constituent pas un avis juridique. Ils ont pour seul but de permettre au lecteur, qui en assume l’entière responsabilité, de les utiliser à des fins qui lui sont propres.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.