Septembre 2020

Mémoire

CI– 033M
C.P. – PL 64
Protection des
renseignements
personnels

PROJET DE LOI 64 :
UNE RÉFORME NÉCESSAIRE,
MAIS DES MESURES MAL ADAPTÉES

CONSULTATIONS PARTICULIÈRES

COMMISSION DES INSTITUTIONS

CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL RCC RETAIL COUNCIL OF CANADA

À PROPOS DU CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

Le Conseil canadien du commerce de détail constitue la principale organisation œuvrant à la défense et à la promotion des intérêts des détaillants.

Fondé en 1963, le Conseil a pour mission d’être la voix des détaillants au Québec et au Canada en offrant un large éventail de services de représentation, de recherche, d’éducation ainsi que d’autres services destinés à favoriser la réussite des détaillants et à mieux faire connaître leur contribution auprès des collectivités et des consommateurs qu’ils servent.

Le Conseil regroupe près de 45 000 établissements au Canada, dont près du tiers sont au Québec. De plus, il est aussi la voix des distributeurs alimentaires du Québec et du Canada. Il s’agit de l’une des plus grandes associations sans but lucratif financées par l’industrie, regroupant tous les types de détaillants tels que les grands magasins, les magasins « grand public », les chaînes spécialisées, les magasins indépendants et les commerces en ligne.

Le commerce de détail est le plus important employeur privé au Canada. Les 2,2 millions de Canadiens qui travaillent dans notre industrie perçoivent des salaires évalués à plus de 60 milliards de dollars et les ventes du secteur ont atteint approximativement 516 milliards de dollars, sans compter les ventes de véhicules et de carburant. Les membres du Conseil canadien du commerce de détail représentent plus des deux tiers des ventes au détail réalisées au Canada.

LE COMMERCE DE DÉTAIL AU QUÉBEC

Au Québec, le commerce de détail est l'employeur de près de 503 000 personnes, soit 11,8 % de la main-d'œuvre. Les deux tiers de ces emplois sont des emplois à temps plein (plus de 30 heures par semaine) et le tiers des emplois sont à temps partiel.

Ce secteur génère des ventes annuelles estimées à 109 milliards de dollars et représente 18,24 milliards de dollars en matière d'activité économique ou 5 % du PIB québécois.

Québec: Le commerce de détail en chiffres

PAGE 1

109 millards $
Le montant total des ventes au detail annuelles au Québec en 2018

33 390 +
Le nombre de magasins au Québec

11,8 %
C'est 503 400 travailleurs canadiens.

1,2 millards $
en immobilisations pour 2018

514 $
Le salaire moyen hebdomadaire pour un employé travaillant à temps plein au sein de notre industrie.

18,24 millards $
Total salaires annuels

COMMERCEDETAIL.ORG

CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

RCC RETAIL COUNCIL OF CANADA

AVANT-PROPOS

Le Conseil canadien du commerce de détail (CCCD) tient tout d'abord à saluer l'initiative de modernisation de cette loi vieillissante. En effet, le contexte numérique dans lequel nous évoluons se métamorphose à une vitesse ahurissante. C'est peut-être un cliché de le répéter, mais c'est important de comprendre que, pour la même capacité technologique d'un simple téléphone intelligent qui réside dans la paume de notre main, un appareil des années 70 occuperait un stade au complet.

Chacun se souvient des premiers enjeux de la révolution numérique où mémoire et capacité de traitement des processeurs étaient au centre des préoccupations des utilisateurs. Aujourd'hui, ces préoccupations ne semblent plus d'actualité ; qui se soucie encore de la mémoire, du processeur et de la vitesse de celui-ci ? Ce qui fait carburer maintenant la révolution numérique, ce sont les données.

Plus précisément, dans le commerce de détail, cette révolution s'est traduite par une accélération et une systématisation de plusieurs pratiques commerciales centenaires. Que ce soit la vente par correspondance pratiquée par les défunts magasins Eaton ou encore les multiples concours postaux, les détaillants ont toujours travaillé afin d'adapter leur offre de service à leur clientèle. Pour les détaillants, le virage numérique n'est pas une révolution culturelle, c'est une simple adaptation des différentes pratiques de l'industrie.

Il y a 100 ans, qui se serait soucié que le siège social d'Eaton se fasse dévaliser et que les responsables de ce larcin se soient emparés des classeurs contenants les commandes des clients ? Dans les années 60, personne ne se serait scandalisé de la disparition d'un sac postal rempli de réponse à un concours organisé par un détaillant, personne sauf les participants à ce concours qui voit leur chance de gagner anéantie.

Le monde a changé, les Arsène Lupin de ce monde ne volent plus des classeurs, mais plutôt des données en s'introduisant frauduleusement dans les systèmes informatiques. La seule donne qui ne change pas, c'est que peu importe les serrures, un voleur déterminé arrivera à ses fins.

Pour des fins d'analyse, nous avons déterminé sept ensembles de mesures contenues dans ce projet de loi.

1. **Circulations transfrontalières des données et équivalence**
2. **Externalisation de la gestion et du traitement des données**
3. **Les questions liées au (x) consentement(s)**
4. **La « dénominalisation » des données et le droit à l'oubli**
5. **La portabilité des données**
6. **Les normes de confidentialité « par défaut »**
7. **Les sanctions administratives et pénales**

À l'ère de la croissance des données, de la numérisation et de l'interconnectivité, il devient de plus en plus important que les cadres législatifs provinciaux et fédéraux sur la protection de la vie privée soient cohérents entre eux afin de soutenir l'économie, les entreprises et les citoyens. Notre société doit tirer parti des innovations technologiques et numériques.

Il est essentiel que toutes les initiatives de réforme des lois sur protection de la vie privée soient mieux harmonisées, sinon nous courons le risque d'être coincé dans une courtepointe de lois sur la protection de la vie privée. Nous invitons donc le législateur québécois à jeter un œil sur les réformes actuellement proposées à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) fédérale.
Un manque d'harmonisation à l'échelle canadienne entraînerait une complexité et des obstacles inutiles pour les entreprises ainsi que des perturbations importantes pour les consommateurs.

Circulation transfrontalière des données et équivalence

Les modifications proposées aux articles 17 et 17.1 exigent qu’une corporation qui cherche à transférer des renseignements personnels à l’extérieur du Québec procède à une évaluation de la protection de la vie privée, y compris une évaluation du cadre juridique de l’État d’accueil. Si l’État d’accueil ne dispose pas d’un cadre juridique équivalent protégeant la vie privée, les renseignements personnels ne peuvent pas être transférés.

Dans sa forme actuelle, le projet de loi 64 ne prévoit aucun mécanisme alternatif pour permettre le transfert de données à l’extérieur du Québec. Nous croyons qu’une entente contractuelle qui serait conforme aux dispositions souhaitées en matière de protection des données combinée avec un cadre de responsabilité adéquat pourrait atteindre les mêmes résultats sans isoler le Québec d’un point de vue numérique.

Le CCCD reconnaît que les auteurs de ce projet de loi se sont appuyés sur les normes les plus récentes et les plus élevées en matière de protection des renseignements personnels. En effet, plusieurs mesures promues par le projet de loi 64 sont largement inspirées du Règlement général sur la protection des données (RGPD) adopté par le Parlement européen le 27 avril 2016. Ses dispositions sont directement applicables dans l’ensemble des 27 États membres de l’Union européenne depuis le 25 mai 2018.

La question de la circulation des données dans le RGPD est à l’image de l’Union européenne elle-même, largement libérale entre les États membres, mais très protectionnistes face au reste du monde. Ce modèle fonctionne bien dans un cadre continental, mais comment pourrait-il fonctionner dans un cadre québécois surtout si aucune autre juridiction nord-américaine n’adhère à ce genre de standard ? Cela reviendrait à tenter de créer des frontières informatiques autour du Québec alors que la tendance est à la libéralisation continentale des échanges commerciaux ; les données étant un élément vital à toute transaction commerciale.

Bien que le RGPD soit une législation modèle en matière de protection des données personnelles, la transplantation de ce modèle au Québec conduirait l’ensemble de la société québécoise dans un isolationnisme informatique non souhaitable.

La clé du succès du RGPD réside dans l’approche continentale découlant de l’application uniforme de cette réglementation par 27 États membres du même ensemble économique et social. Dans un contexte nord-américain, l’imposition d’une obligation d’analyse sur l’impact en matière d’équivalence fera porter un fardeau excessif, voire déraisonnable, sur le dos des petits et des grands entrepreneurs.

Ce qu'il faut retenir :

- L'exigence d'équivalence crée un nouvel obstacle important pour les entreprises québécoises, en particulier les PME, ce qui réduira la capacité des entreprises québécoises de faire face à la concurrence nord-américaine, tout en réduisant l'éventail des choix pour le consommateur.
- L'exigence d'équivalence risque de mettre le Québec en porte à faux avec les dispositions de l'accord commercial sur les flux transfrontaliers de données, tout comme l'exigence d'avoir des installations informatiques locales comme condition de faire des affaires.
- Si l'exigence d'équivalence est maintenue, d'autres mécanismes doivent être mis en place pour permettre le transfert de renseignements personnels à l'extérieur du Québec vers des juridictions non équivalentes. Le RGPD a un processus d'équivalence et des méthodes alternatives quant au transfert vers des États sans équivalence. Dans un cas comme celui-là, le RGPD exige une approche de conformité réglementaire contractuelle plutôt qu'une approche fondée sur un cadre légal équivalent.

Modifications recommandées

Avant de communiquer des renseignements personnels à l'extérieur du Québec, une personne exerçant une entreprise doit procéder à une évaluation des facteurs liés à la vie privée, et doit en particulier tenir compte de :

1) la sensibilité de l'information ;
2) les fins pour lesquelles il doit être utilisé ; et
3) des mesures de protection qui s'appliqueraient à elle, y compris les mesures contractuelles.

Les renseignements peuvent être communiqués si l'évaluation établit que ceux-ci bénéficieraient d'un niveau de protection comparable au moyen de mesures législatives, contractuelles ou autres équivalentes aux protections offertes en vertu de la présente loi. La communication des informations doit faire l'objet d'un accord écrit qui tient compte notamment des résultats de l'évaluation et, le cas échéant, des conditions convenues pour atténuer les risques identifiés dans l'évaluation.

Il en va de même lorsque la personne exerçant une entreprise confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver ces renseignements en son nom.

Nous suggérons donc de modifier l'article 17 pour (i) supprimer l'exigence d'évaluation d'équivalence obligatoire et permettre des protections contractuelles adéquates (celle-ci pouvant être encadré par la loi) pour le transfert de renseignements personnels hors du Québec, comme le prévoit le RGPD, et ce qui rendrait caduque la référence liste ministérielle de juridictions équivalentes prévues au projet de loi.

Externalisation de la gestion et du traitement des données

Où commence la responsabilité en matière de gestion et de traitement des données personnels et où s'arrête-t-elle ? Telle est la question ici. Le projet de loi à l'étude introduit *de facto* la notion de « *primo collecteur de données* » et lui incombe la responsabilité des données collectées dans le cadre de ses activités.

Selon notre compréhension de cette disposition, et advenant le cas où cette section de la nouvelle loi aurait été en vigueur, les multiples détaillants, grands et petits, auraient pu être mis à l'amende et tenus responsables dans l'affaire de la fuite de données chez Desjardins.

Le projet de loi 64 devrait préciser que, dans une relation d'impartition ou de vis à vis, le principal (c'est-à-dire « une personne qui exerce une entreprise ») est le seul responsable à veiller au respect de la loi sur la protection des renseignements personnels. Le rôle de l'agent et/ou du fournisseur de services (c'est-à-dire « une personne ou un organisme exerçant un mandat ou effectuant un contrat d'entreprise ou de services ») est de suivre les instructions de son client. Le mandataire ou le contractuel doit mettre tout en œuvre pour protéger les données qui lui sont confiées. Les ententes contractuelles prévoient d'ailleurs ce genre de chose.

L'article 18.3 reconnaît implicitement les rôles et les responsabilités distincts que jouent diverses organisations dans l'écosystème des données. La responsabilité incombe à l'organisation qui contrôle en fin de compte les renseignements personnels recueillis, comment ils sont utilisés et à quelles fins, avec qui ils sont partagés et comment ils sont traités. Le projet de loi 64 limite implicitement les obligations de l'agent qui fournit des services à la personne exerçant une entreprise (appelée « *personne ou organisme exerçant un mandat ou effectuant un contrat d'entreprise ou de services* ») aux obligations énoncées à l'article 18.3.

Les agents ou les fournisseurs de service sont tenus de suivre les instructions de leur directeur. Les fournisseurs de services ont une possibilité de protéger adéquatement les renseignements personnels, mais ces responsabilités sont généralement définies dans le contrat entre eux et leurs clients.

Des éclaircissements sont également nécessaires tout au long du projet de loi 64 sur la question de savoir si l'utilisation des mots « *une personne* » ou *« une personne ou un organisme* » est censée s'appliquer au responsable du traitement des données ou à un sous-traitant. Voir par exemple les sections 1.1, 8, 8.1, 8.2, 16, 18.3, 21, 36, 53 et 91.

Changement recommandé

Pour éviter toute confusion quant aux responsabilités des parties, nous recommandons d’ajouter la disposition suivante au projet de loi 64 :

« 18,3 (3) Aux fins de la présente loi, une personne ou un organisme exerçant un mandat ou effectuant un contrat d’entreprise ou pour des services pour le compte d’une personne exerçant une entreprise n’est pas considéré comme une personne exerçant une entreprise. »

Les questions liées aux consentements

Le projet de loi 64 apporte plusieurs clarifications attendues au cadre de consentement pour les renseignements personnels. Ces clarifications réduisent le fardeau des processus opérationnels et reflètent mieux les attentes des consommateurs. Malheureusement, le projet de loi introduit également d’autres obligations de consentement ciblé peu pratiques qui auront pour conséquence involontaire de créer une « *fatigue du consentement* » chez les consommateurs et de réduire la valeur réelle du consentement en tant que protection de la vie privée.

Toutefois, le libellé entourant l’utilisation de formes appropriées de consentement dans le projet de loi 64 est ambigu. Par exemple, le projet de loi semble exiger le consentement dans pratiquement tous les cas où des renseignements personnels sont utilisés ou transférés à un tiers à la suite des articles 12 et 13. L’article 14 indique que ce consentement doit être clair, libre, informé, donné à des fins spécifiques et doit être demandé à chacun de ces fins, dans un langage clair, simple et séparé de toute autre information fournie à la personne concernée.

Ces exigences devraient être ajustées selon les nombreuses circonstances. La portée générale du libellé est incompatible avec le rôle important joué par le consentement implicite. Les alternatives limitées ou les exceptions communes au consentement créeront un fardeau inutile pour les entreprises et pourront engendrer une fatigue du consentement pour les consommateurs qui se traduirait par une perte d’attention du citoyen qui nuirait à l’objet recherché, soit un consentement éclairé.

Le projet de loi 64 ne fait pas actuellement référence aux concepts de consentement exprès et implicite, contrairement à d’autres lois sur la protection de la vie privée au Canada, qui autorisent le consentement implicite dans certaines circonstances. Le projet de loi stipule qu’un consentement exprès est requis en ce qui concerne les informations personnelles sensibles, cependant

Le CCCD appuie les exceptions proposées à l’exigence de consentement pour :

- Le transfert de renseignements personnels à un agent pour traitement (s. 18.3) ;
- Les utilisations secondaires et l’analyse d’entreprise lorsque l’utilisation est compatible avec le consentement original (art. 12 [1]) ;

- Lorsque l'utilisation est clairement dans l'intérêt supérieur de l'individu (s. 12 [2]) ;
- Une transaction commerciale (s.18.4).

Le CCCD est d'accord aussi avec l'exclusion des coordonnées commerciales de la définition de renseignements personnels qui déclencheraient l'obligation de consentement (s.1). Par ailleurs, nous aimerions qu'il soit précisé que le consentement implicite est suffisant lorsqu'il est raisonnable dans les circonstances.

En outre, il convient d'envisager des exceptions supplémentaires au consentement ou aux autorités légales pour le traitement des données personnelles, comme dans le RGPD en vertu duquel le consentement n'est que l'une des six bases légales et valides pour le traitement des données personnelles.

Modifications recommandées

14. Lorsque le consentement explicite *est approprié* en vertu de la *présente loi,* ce consentement doit être *clair, libre et informé* et être donné à des *~~fins spécifiques~~. Il doit être demandé* à *~~chaque fin,~~ dans un langage clair et simple ~~et séparément de toute autre information fournie à la personne concernée~~. Si la personne concernée en fait la demande, une assistance est fournie pour l'aider à comprendre la portée du consentement demandé.*

Le consentement d'un mineur de moins de 14 ans est donné par la personne ayant l'autorité parentale.

.

Le consentement d'un mineur de 14 ans ou plus est donné par le mineur ou par la personne ayant l'autorité parentale.

~~Le consentement n'est valable que pour le temps nécessaire pour atteindre les fins pour lesquelles il a été demandé.~~
~~Le consentement qui n'est pas donné conformément à la présente loi est sans effet.~~

La « dénominalisation » des données et droit à l’oubli

L’article 23 du projet de loi précise que des renseignements personnels sont dénominalisés, lorsqu’irréversiblement, ils ne permettent plus à la personne d’être identifiée directement ou indirectement. Il s’agit d’une norme très élevée à respecter et qui ne tient pas compte de la manière dont les renseignements personnels peuvent actuellement être dénominalisés et protégés, par l’utilisation de la technologie (par exemple, par l’utilisation de jetons, de segmentations, etc.).

Il faut bien comprendre que, dans le commerce de détail, toutes les transactions sont rattachées à un client et que les systèmes sont intégrés (incluant les programmes de fidélité). Il est donc fiscalement impossible de faire disparaitre toute référence nominative des systèmes informatiques des détaillants. Cela reviendrait à forcer les détaillants à ne plus se conformer aux lois fiscales qui exigent de garder une trace de toutes les transactions aux fins de vérification ultérieure.

De plus, il faut aussi tenir compte du fait que dans de nombreuses enquêtes criminelles portant justement sur des fraudes informatiques commises par certains individus, il pourrait être utile pour les procureurs de pouvoir « *ressusciter* » l’identité du fraudeur. L’article 23, tel que libellé actuellement, pourrait donc dans certains cas permettre à un contrevenant de forcer la disparition de preuves incriminantes.

Modification recommandée

L’utilisation de la norme de « irréversible » est trop élevée pour maintenir une utilisation efficace des renseignements personnels par les entreprises, sans compter sur l’effet de nuisance qu’il pourrait induire dans certaines enquêtes criminelles. Nous proposons donc de retirer le mot « *irréversiblement* » afin de sursoir aux effets indésirables que cette notion induit.

Nous proposons également de retirer les mots « i*ndirectement* » du même libellé, pour préciser qu’une autre partie détenant les consentements appropriés peut renominaliser les données avec toutes les réserves et pour toutes les raisons énoncées plus haut.

Portabilité des données

Bien que la portabilité des données offre certains avantages tant aux consommateurs qu'aux entreprises, elle comporte des risques inhérents à la protection des consommateurs, à la protection de la vie privée et à la confidentialité, à la cybersécurité, à la diminution de l'innovation et à la concurrence. Une étude approfondie de la mécanique de la portabilité des données et de ses répercussions non liées à la protection de la vie privée est nécessaire avant que les mesures énoncées à l'article 27 du projet de loi 64 puissent être mises en œuvre.

Au-delà du droit existant pour les particuliers de demander l'accès aux renseignements personnels que les entreprises détiennent à leur sujet, la portabilité des données permettrait aux particuliers d'obtenir leurs renseignements personnels et de les transférer entre les organisations s'ils le souhaitent.

La portabilité des données pourra améliorer l'autonomie individuelle, la protection de la vie privée et le choix des consommateurs si elle est mise en œuvre correctement. Cependant, il y a de nombreux défis pratiques. Si ces défis ne sont pas relevés adéquatement, les répercussions sur les individus pourraient se traduire par une réduction de sécurité en matière de renseignements privés et un risque accru de fraude.

Une architecture robuste pour soutenir la portabilité des données est nécessaire et peut varier d'un secteur à l'autre. Le gouvernement devrait adopter une approche progressive de la portabilité des données au fur et à mesure que l'infrastructure et les technologies se développent.

En termes de portabilité, le droit ne devrait s'appliquer qu'entre la personne et l'organisation ; les organisations tierces ne devraient pas être habilitées à exercer le droit de portabilité au nom d'un individu. Une divulgation de données pourrait être autorisée entre des organisations lorsque l'organisation destinataire a un droit légal de collecter les informations personnelles, et ce uniquement à la demande et avec le consentement exprès de l'individu. Une telle disposition permettrait de réduire le risque de fraude et de vol d'identité.

Les données couvertes par ce droit devraient être limitées aux renseignements que la personne a fournis à l'organisation. Ce droit ne devrait pas s'appliquer à d'autres formes de données dont les entreprises sont propriétaires et que ne sont pas facilement exportable ou encore qui font l'objet d'informations concurrentielles.

Par exemple :

- Données dérivées provenant d'informations commerciales et des données observées ;
- Données dénominalisées ;
- Non propice à la portabilité en raison du format (notes d'appel, plaintes, etc.)

Autre sujet d'inquiétudes pour les détaillants, comment trace-t-on la frontière des responsabilités lors du transfert d'information, que ce soit vers le consommateur ou une autre société autorisé à recevoir les données. Si cet élément n'est pas clarifié, il pourrait s'ensuivre des situations où il deviendrait difficile de départager la responsabilité légale en cas de non-conformité ou de poursuite judiciaire.

Il faut réfléchir attentivement pour éviter les atteintes à la protection des données et l'exposition à la fraude, ainsi qu'au niveau approprié d'authentification des données (éventuellement liées à la sensibilité des données) et à leur chiffrement. Le format informatique approprié pour que les individus reçoivent leurs données devrait également être déterminé. La Loi devrait aussi établir les bases sur lesquelles une organisation peut s'opposer à une demande de portabilité des données.

Modification recommandée

La mise en œuvre d'un droit de portabilité des données devrait être reportée en attendant que le gouvernement approfondisse les mécanismes d'un tel droit et des répercussions non liées à la protection de la vie privée. Les secteurs de l'industrie devraient être engagés à identifier toute considération technique ou concurrentielle spécifique. Le droit lui-même devrait être introduit de manière progressive et l'harmonisation devrait être un objectif de maximiser tous les avantages et de limiter la confusion et la complexité inutile.

Les normes de confidentialité « par défaut »

Le projet de loi 64 contient des mesures visant à maximiser la sécurité et la confidentialité des renseignements personnels, souvent connues sous le nom de sécurité par défaut et de protection de la vie privée par défaut, tel qu'indiqué dans les articles 3.1, 3.2 et 9.1. Toutefois, ces mesures telles que libellées manquent de précision et pourraient avoir des répercussions négatives sur les consommateurs si elles sont appliquées sans tenir compte des circonstances, des risques ou de la sensibilité des informations personnelles.

Le projet de loi 64 exige des organisations qu'elles « protègent les renseignements personnels détenus par une personne » (p. 3.1) et qu'elles établissent et mettent en œuvre des politiques et des pratiques de gouvernance qui « assurent » la protection de ces renseignements (s. 3.2).

Les normes de sécurité de l'information énoncée aux articles 3.1, 3.2 et 9.1 sont incompatibles avec les exigences qualifiées énoncées à l'article 10 de la Loi qui prévoit que les organisations doivent mettre en œuvre des mesures de sécurité qui sont « *raisonnables compte tenu de la sensibilité de l'information, des fins pour lesquelles elles doivent être utilisées, de la quantité et de la distribution de l'information et du moyen sur lequel elles sont stockées* » (s. 10).

Les lois équivalentes au Canada qualifient les obligations de protection de l'information imposées aux organisations en obligeant les organisations à mettre en œuvre des mesures de protection « raisonnables » et « appropriées » dans les circonstances. De même, la norme de sauvegarde du RGPD exige « *des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au risque* ». Nous croyons que le projet de loi 64 devrait suivre une approche similaire.

Le projet de loi 64 exige également que les organisations qui recueillent des renseignements personnels lorsqu'elles « *offrent un produit ou un service technologique s'assurent que les paramètres du produit ou du service fournissent le plus haut niveau de confidentialité par défaut, sans aucune intervention de la personne concernée* » (s. 9.1). Cette clause de « *confidentialité par défaut* » est d'une portée beaucoup plus large et beaucoup plus stricte que le concept de « *conception à des fins de vie privée* » dans le cadre du RGPD, qui exige que celui qui est le contrôleur des données mette en œuvre des « mesures techniques et organisationnelles appropriées » pour la mise en œuvre efficace des principes de protection des données, en tenant compte de la nature, de la portée, du contexte, des risques et des objectifs du traitement. (Art. 25 [1]). De même, le RGPD exige des contrôleurs de données qu'ils mettent en œuvre des mesures techniques et organisationnelles « *appropriées* » pour s'assurer que, par défaut, « *seules les données à caractère personnel nécessaires à chaque fin spécifique du traitement sont traitée*s » (art. 25 [2]).

Le CCCD appuie une approche souple de l'exigence de confidentialité, de sorte que le niveau de confidentialité et les coûts et processus connexes soient proportionnels à la sensibilité des renseignements personnels et au contexte de la relation. Une application stricte de l'exigence de confidentialité pourrait conduire inutilement à de mauvaises expériences de consommation. De nombreux appareils et services sont programmés pour être « intelligents » afin d'assurer l'accès aux informations nécessaires pour l'accès aux besoins du consommateur afin d'offrir les services que le consommateur attend. Lire, littéralement, la disposition de confidentialité pourrait exiger que tous les services et les appareils soient préprogrammés à la confidentialité maximale dès le départ, ce qui serait virtuellement impraticable et exigerait parfois une longue programmation pour le consommateur afin de lui permettre d'accéder aux services auxquels il s'attend.

Modifications recommandées

Le CCCD appuierait fortement une approche souple de l'exigence en matière de sécurité, de sorte que le niveau de sécurité et les coûts et de processus connexes soient proportionnels à la sensibilité des renseignements et à la nature de ceux-ci, au contexte, aux risques et à la finalité du traitement. Nous tenons d'ailleurs à souligner le fait que le RGPD a évolué sur cette question et que les normes européennes telles que rédigées aujourd'hui sont beaucoup plus flexibles que les normes proposées ici.

L'obligation à l'article 3.2 de publier des politiques relatives au traitement des renseignements personnels est raisonnable, mais devrait être formulée plus clairement pour exclure les politiques et procédures internes. De nombreuses politiques internes et processus sont propres aux entreprises et sensibles à la concurrence, elles ne sont pas écrites dans un langage destiné aux consommateurs. La publication de politiques internes sur la confidentialité pourrait même parfois aider les fraudeurs.

Finalement

Les sanctions administratives et pénales

Le projet de loi 64 crée un nouveau régime de sanctions administratives et pénales qui nous apparait disproportionné. Ce nouveau régime n'apporte aucune garantie sur les procédures administratives pouvant conduire à des sanctions administratives. De plus, tel que décrit plus haut dans la section « L'externalisation de la gestion et du traitement des données », la frontière de responsabilité légale étant mal établie, ce régime de sanction pourrait résulter en des situations iniques et surtout absurdes.

Les mesures d'application proposées par le projet de loi 64 comprennent des amendes pouvant aller jusqu'à 25 000 000 $ ou un montant correspondant à 4 % du chiffre d'affaires mondial pour l'exercice précédent. Pour une infraction subséquente, les amendes seraient doublées. Le projet de loi prévoit également des sanctions administratives financières pouvant aller jusqu'à 10 000 000 $ ou 2 % du chiffre d'affaires mondial pour l'exercice précédent. De plus, le projet de loi propose un droit de poursuite privé onéreux sans responsabilité.

Ici, il faut faire la distinction entre une sanction administrative et une sanction pénale. Dans le cas d'une sanction administrative, il est de notoriété publique que le fardeau de la preuve est renversé. Les autorités constatent le manquement et émettent la sanction administrative et c'est au défendeur de contester le manquement et la sanction au tribunal administratif (TAQ). Les sanctions administratives amènent un effet pervers (qui est mitigé dans le cas d'une sanction raisonnable). Même en cas de contestation devants le TAQ, le montant de la sanction doit être porté au passif de la compagnie, et souvent les délais d'auditions au TAQ peuvent s'étendent sur plus d'un an. Dans les cas où la sanction serait substantielle, cette charge au passif de la corporation pourrait se traduire par une faillite technique de la corporation alors que sa culpabilité ou son innocence n'aurait pas encore été confirmée par un tribunal.

Pour ce qui est de sanctions pénales, un procès devant être tenu avant l'application des sanctions, la culpabilité sera donc démontrée avant l'application de telles sanctions. De plus, le système judiciaire verra à ce que la sanction soit proportionnelle à l'offense.

Le CCCD est très préoccupé par le fait que la fourchette maximale des sanctions administratives et pénales soit excessive et pourrait ne pas être proportionnel aux cas particuliers. Ce nouveau régime pourrait conduire plusieurs entreprises à hésiter à s'installer au Québec. Si le montant maximal des sanctions administratives devait être maintenu, le projet de loi doit prévoir un régime procédural distinct du régime de procédure administrative qui prévaut actuellement au gouvernement du Québec. Il est inconcevable que, juridiquement parlant, des sanctions d'une telle ampleur soient « payables sur-le-champ » sans autre forme de procès.

La rédaction actuelle sous-tend une responsabilité sans égard à la faute. Dans la majorité des cas, la responsabilité de l'entreprise s'attache moins à l'évènement sous-jacent, qui est souvent impossible à prévoir et impossible à éviter, qu'aux moyens pris par l'entreprise pour protéger les données. Autrement dit, une entreprise qui a agi de façon responsable et prévoyante ne devrait pas être tenue responsable pour un évènement hors de son contrôle.

Malheureusement, le projet de loi ne reconnaît pas la notion de diligence en matière de protection des données et fait porter l'ensemble de la responsabilité au « primo détenteur de ces données ».

Donc, même en prenant toutes les précautions possibles pour gérer les renseignements personnels de façon sécuritaire et conforme, un détaillant pourrait tout de même être accusé dans le cas d'un *hacking* de haut niveau dont même les gouvernements ne peuvent se protéger. Bref, ce niveau strict de responsabilité en matière de protection de la vie privée est sans précédent et créerait un fardeau déraisonnable pour les entreprises qui exercent leurs activités au Québec.

Finalement, à ce chapitre il est primordial d'assurer une harmonisation avec les autres législations canadiennes de protection des renseignements privés, afin d'éviter des situations où la même « faute » pourrait être sanctionnée plusieurs fois, que ce soit au niveau des autres provinces ou au niveau fédéral.

Modifications recommandées

Les dispositions relatives à l'application et aux sanctions devraient être réexaminées et rédigées à nouveau. Le CCCD recommande que :

1. L'utilisation d'un pourcentage du chiffre d'affaires mondial dans le calcul du régime de sanctions administratives et pénales devrait être abandonnée.
2. Les montants maximaux prévus dans le régime de sanction administrative et pénale devraient être revus à la baisse.
3. Tout régime de responsabilité, sans égard à la faute, devrait permettre tous les moyens de défense raisonnables en droit, y compris l'exercice de la diligence raisonnable.

CONCLUSIONS

Bien que le CCCD considère qu'une modernisation de la Loi soit essentielle à ce moment-ci, nous croyons toutefois qu'il faille revoir et adapter bon nombre des mesures proposées. L'univers dans lequel nos détaillants évoluent dépasse les limites physique et juridique du Québec. L'adoption de ce projet aurait pour effet de créer des contraintes législatives uniques au monde. Ce que le gouvernement du Québec met de l'avant, c'est un cadre législatif plus sévère que le RGPD duquel il est inspiré et ce, sans tenir compte des adaptations issues du test de réalité qu'a connu le RGPD entre son édiction et aujourd'hui.

Dans une perspective de compétitivité et d'ouverture vers les marchés extérieurs au Québec, ce projet de loi impose une norme qui n'est pas compatible avec le reste du marché naturel de nos détaillants. C'est un peu comme si le Gouvernement du Québec décidait d'importer les normes électriques européennes ici au Québec, alors que ces normes ne sont pas compatibles avec l'Amérique du Nord.

En conclusion, nous avons fait beaucoup de recommandation section par section, mais nous souhaitons faire une recommandation transversale :

« Que le gouvernement du Québec mette sur pied un comité fédéral/provincial afin d'en venir à l'élaboration de normes pancanadienne sur la protection des renseignements personnels. »

Pour plus d'informations :

Septembre 2020

Jean François Belleau
Directeur relations gouvernementales, Québec
Tél. : 514.982.0267 | 1.877.229.0922 **Poste** 332
Courriel : jfbelleau@cccd-rcc.org

Conseil canadien du commerce de détail
550, rue Sherbrooke Ouest, Bureau 1680, Tour Ouest | Montréal (Québec) | H3A 1B9
Tél. : (514) 982-0267 | Sans frais: (877) 229-0922