BAC IBC | Bureau d'assurance du Canada
Insurance Bureau of Canada

Mémoire sur le projet de loi n°64
Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Présenté à la

Commission des institutions

Assemblée nationale du Québec

Septembre 2020

BAC IBC | Bureau d'assurance du Canada
Insurance Bureau of Canada

Le Bureau d'assurance du Canada est l'association qui représente les sociétés privées d'assurance de dommages. L'industrie de l'assurance de dommages joue un rôle de premier plan dans l'économie québécoise en permettant à la population de se prémunir contre des sinistres pouvant avoir un impact important sur sa sécurité financière en protégeant son patrimoine.

Pour mener à bien sa mission, le BAC :

- Maintient des relations suivies avec le gouvernement, les consommateurs et toute autre partie concernée;
- Intervient dans des dossiers règlementaires et législatifs;
- Fait équipe avec le gouvernement et avec divers intervenants dans des initiatives de prévention;
- Informe le grand public en matière d'assurance, tant dans le quotidien qu'en situation de crise;
- Élabore des campagnes d'éducation et de sensibilisation à l'intention des consommateurs.

Le BAC est non seulement le porte-parole de l'Industrie, mais aussi un précieux partenaire pour les gouvernements, les intervenants du milieu de l'assurance de dommages, et les consommateurs.

Bureau d'assurance du Canada
1981, avenue McGill College, bureau 620
Tour Richter
Montréal (Québec) H3A 2Y1

Septembre 2020

TABLE DES MATIÈRES

INTRODUCTION

Au nom de ses membres, le Bureau d'assurance du Canada (BAC) tient à souligner l'ampleur du travail accompli par le ministère de la Justice pour moderniser la *Loi sur la protection des renseignements personnels dans le secteur privé* (*Loi sur le secteur privé*) qui n'a pas connu de réforme depuis son adoption.

Le présent mémoire se veut un résumé de la position des assureurs de dommages relativement aux modifications et aux nouveaux droits accordés par le projet de loi n° 64 (PL64) aux personnes concernées. Il vise à vous informer des problématiques liées à l'application de certains articles pour notre industrie. Plus particulièrement, l'industrie de l'assurance de dommages est préoccupée par :

- Les critères applicables aux incidents de confidentialité qui ne sont pas harmonisés avec ceux des autres lois en matière de protection des renseignements personnels et manquent de clarté;
- Le montant des sanctions administratives pécuniaires et des sanctions pénales qui ne reflète pas le marché québécois;
- Les mécanismes proposés pour le transfert d'informations dans d'autres juridictions qui imposent d'importantes barrières aux entreprises;
- Le retrait d'exceptions importantes pour l'industrie, notamment celles prévues aux articles 22 à 26 de *Loi sur le secteur privé* incluant celle concernant les listes nominatives;
- Le traitement automatisé de l'information et les droits y afférant en vertu de l'article 12.1 du PL64, qui devrait prévoir certaines exceptions;
- Les dispositions transitoires qui prévoient une entrée en vigueur très rapide et qui ne prévoient pas de droits acquis pour les consentements obtenus avant cette entrée en vigueur.

COMMENTAIRES GÉNÉRAUX

Harmonisation à travers le Canada

Le PL64 s'inspire des normes européennes en matière de protection des renseignements personnels, notamment du *Règlement général sur la protection des données* (RGPD)[1]. Ce règlement a inspiré plusieurs autres juridictions à moderniser et à adopter des règles semblables et son succès repose, entre autres, sur l'harmonisation de la protection des renseignements personnels à travers l'Union européenne, ce qui permet le libre flux des renseignements personnels à travers le marché européen. Ce succès n'aurait pas eu lieu sans une vision commune de la protection des renseignements personnels, si critique pour les entreprises, et qui permet d'éviter des obstacles artificiels entre juridictions.

Pour que le PL64 puisse obtenir un succès comparable à celui du RGPD, le BAC est d'avis que les dispositions doivent refléter le marché québécois, mais également s'harmoniser avec les dispositions canadiennes, notamment celles prévues à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[2]. Cette harmonisation permettra d'éviter de créer des difficultés d'application pour les entreprises ou les groupes financiers qui œuvrent à travers le Canada. On peut penser aux incidents de confidentialité, qui ne se limitent pas aux

[1] Règlement (UE) 2016/679
[2] LC 2000, c 5.

frontières du Québec, ou encore à la détention de renseignements créés par des organismes fédéraux, par exemple le numéro d'assurance sociale, qui requiert un traitement harmonisé entre les provinces. Il importe que le gouvernement du Québec maintienne une coordination étroite avec le gouvernement fédéral et les gouvernements des autres provinces afin de s'assurer que la réglementation relative à la protection des renseignements personnels soit harmonisée au Canada. Cette harmonisation est nécessaire dans la mesure où la plupart des institutions financières maintiennent des opérations au niveau national. Il en va aussi de l'intérêt des consommateurs québécois qui bénéficieront d'une réglementation harmonisée. Malheureusement, dans sa mouture actuelle, le PL64 ne semble pas s'arrimer avec les autres législations en matière de protection de renseignements personnels, incluant la LPRPDE.

Encadrement des assureurs par l'Autorité des marchés financiers

Les assureurs ont mis en place des règles de gouvernance afin d'être conformes aux lignes directrices de l'Autorité des marchés financiers (l'Autorité) et du Bureau du surintendant des institutions financières. Or, à plusieurs endroits dans le PL64, les obligations attendues des entreprises sont très précises et entrent en conflit avec l'encadrement de l'Autorité qui vise spécifiquement les institutions financières. C'est le cas notamment quant aux rôles et responsabilités attribués au responsable de la protection des renseignements personnels dans la *Ligne directrice sur la gestion de risques liés aux technologies de l'information et aux communications*[3]. C'est également le cas des obligations relatives aux incidents de confidentialité, pour lesquels l'Autorité a émis des exigences qui s'harmonisent difficilement avec les exigences prévues au PL64.

De plus, le BAC est d'avis que le PL64 ne devrait pas cibler les stratégies pour atteindre un résultat, mais bien le résultat attendu des entreprises. Une telle approche augmente l'efficacité et l'efficience de la gouvernance qui nécessite des dispositifs de gestion de risques et de contrôle répartis entre plusieurs secteurs et niveaux de l'organisation. À cette fin, le respect de la nature, de la taille, de la complexité et du profil de risque de l'entreprise doit être considéré. Il s'agit du principe de la proportionnalité qui est nécessaire pour permettre à une entreprise de se développer dans le respect de sa culture et de ses moyens.

Le BAC suggère donc que le PL64 soit basé sur des principes, non des exigences spécifiques et rigides, de manière à donner aux institutions financières la flexibilité nécessaire pour mettre en œuvre les principes, en considération de leur modèle d'affaires spécifique.

Renseignements personnels des employés de l'entreprise

Le PL64 ne différencie pas les renseignements personnels qui concernent des tiers de ceux qui concernent les employés d'une entreprise. Or, la relation qu'une entreprise a avec un tiers est complètement différente de celle qu'elle a avec un employé.

Le BAC recommande d'introduire une exception pour les renseignements personnels concernant les employés d'une entreprise et d'introduire un article semblable aux articles 7.3 et 7.4 de la LPRPDE qui permet de collecter, d'utiliser et de communiquer des renseignements personnels sans le consentement de la personne concernée si cela est nécessaire pour établir ou gérer la relation d'emploi.

[3] Par exemple, l'Autorité précise plusieurs rôles et responsabilités qui devront être attribués à des hauts dirigeants ou à des comités concernant la protection et la gestion des renseignements personnels notamment à la page 13.

Échange de renseignements personnels entre entités du même groupe

Plusieurs assureurs sont constitués en groupes financiers et certains dirigeants peuvent avoir un rôle dans différentes entités du groupe. Afin de considérer cette réalité, **le BAC recommande que le PL64 crée une exception pour la communication des renseignements personnels à l'intérieur d'un même groupe financier.**

COMMENTAIRES SPÉCIFIQUES

SECTION I.1
RESPONSABILITÉS RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Article 3.1

L'article 3.1 du PL64 introduit le principe de responsabilité et désigne d'office la personne ayant la plus haute autorité au sein de l'entreprise pour exercer les fonctions de responsable de la protection des renseignements personnels. **Le BAC recommande de préciser que c'est la personne ayant la plus haute autorité au Québec qui est responsable d'office**.

L'alinéa 2 de l'article 3.1 prévoit que le responsable des renseignements personnels peut déléguer cette fonction à un membre du personnel. Le BAC considère qu'il serait également important de permettre la sous-délégation de l'exécution de ces fonctions à un membre du personnel au Québec ou à l'extérieur du Québec. En effet, le PL64 attribue une liste importante de fonctions que devra assumer le responsable. Par exemple, les articles 30, 32, 34 et 35 du PL64 sont rédigés de façon à assigner exclusivement au responsable de la protection des renseignements personnels les obligations de répondre aux demandes d'accès ou de rectification et de prêter assistance aux consommateurs. Si la Loi ne permet pas la sous-délégation, cela risque d'alourdir le processus de demande d'accès en plus d'empêcher les consommateurs de bénéficier d'un service optimal. Ces fonctions ne peuvent pas toujours être exécutées de manière optimale par une seule personne. Conséquemment, il est important que l'exécution des obligations du responsable puisse être effectuée par une autre personne, ou secteurs opérationnels, afin de laisser la latitude nécessaire au développement d'une gouvernance optimale.

D'une part, les compétences nécessaires pour les effectuer sont diverses et peuvent être spécifiques. Par exemple, des connaissances en technologie de l'information peuvent être requises. D'autre part, la sous-délégation est importante afin de permettre le respect de la structure organisationnelle des entreprises et d'éviter que plusieurs personnes qui ont des fonctions déléguées se rapportent directement à la personne ayant la plus haute autorité. Le BAC est d'avis que seule la personne déléguée par la personne ayant la plus haute autorité devrait se rapporter à celle-ci.

Considérant ce qui précède, le BAC est d'avis qu'il serait préférable de se limiter à la désignation d'une personne responsable et imputable, tout en laissant le soin aux entreprises d'adopter le cadre approprié pour assurer le respect de la loi.

Aussi, contrairement au RGPD[4] qui prévoit la mutualisation des fonctions du responsable de la protection des renseignements personnels entre plusieurs entités, le PL64 est muet à cet égard. Plusieurs compagnies d'assurance font partie d'un même groupe financier et gèrent leurs

[4] Article 37(2)

activités de façon intégrée, elles pourraient donc bénéficier de la mutualisation du rôle de responsable.

Finalement, le PL64 permet uniquement la délégation du responsable de la protection des renseignements personnels à un membre du personnel. Considérant l'importance des fonctions qu'exécutera ce responsable et les compétences requises pour bien y parvenir, il peut s'avérer judicieux de permettre qu'elles soient exécutées par une personne externe à l'organisation. Ceci peut être requis notamment lorsque l'entreprise n'a pas d'employé détenant les compétences nécessaires sur une base temporaire[5] ou permanente. D'ailleurs, cette délégation à une personne externe de l'organisation est permise en vertu du RGPD dans la mesure où cette délégation s'effectue par l'octroi d'un contrat de service[6].

Si le PL64 ne prévoit pas la sous-délégation suggérée, il est à craindre que les demandes formulées par les consommateurs ne puissent pas être satisfaites de façon efficiente, ce qui serait au détriment des consommateurs, particulièrement dans les grandes entreprises où le volume de telles demandes peut s'avérer important.

Le BAC recommande ainsi de modifier l'article 3.1 pour :

- Préciser que le responsable de la protection des renseignements personnels puisse déléguer, en tout et en partie, ses fonctions à d'autres personnes ou unités d'affaires tout en demeurant imputable;
- Préciser que la personne ayant la plus haute autorité au Québec est la personne responsable;
- Permettre la mutualisation des fonctions de responsable de la protection des renseignements personnels afin qu'un groupe d'entreprises puisse désigner un seul responsable de la protection des renseignements personnels pour les activités du groupe;
- Permettre la délégation à une personne externe à l'entreprise dans la mesure où cette délégation s'effectue conformément à un contrat de service écrit.

Article 3.2

L'article 3.2 exige que les politiques encadrant sa gouvernance à l'égard des renseignements personnels soient publiées sur le site internet de l'entreprise. Le BAC reconnaît l'importance du principe de transparence avec les consommateurs. Toutefois, il est d'avis que la publication de toutes les politiques de gouvernance n'est pas nécessaire pour y arriver, d'autant plus que ces politiques sont généralement destinées au personnel de l'entreprise ou à ses fournisseurs.

Cette publication peut également créer des enjeux de concurrence et pourrait même permettre à des personnes mal intentionnées de trouver des zones de vulnérabilité.

Finalement, le BAC considère que la publication des politiques de gouvernance n'offre aucune valeur ajoutée pour les consommateurs dans la gestion de ses renseignements personnels et que l'obligation prévue à l'article 8.2 du PL64 se limitant à publier une politique de confidentialité dédiée aux consommateurs sur le site internet de l'entreprise est suffisante. En effet, le BAC croit que les consommateurs désirent d'abord et avant tout connaître la politique des entreprises en ce qui concerne la cueillette, l'utilisation et la communication de leurs

[5] Une situation temporaire pourrait être le départ du responsable et son poste se retrouvant vacant.
[6] Article 37(6)

renseignements personnels et la manière dont ces renseignements sont protégés, et non les politiques et procédures de gouvernance internes.

Article 3.3

L'article 3.3 impose d'effectuer une évaluation des facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services. Tel que rédigé actuellement, cette disposition encadre le processus et non le résultat attendu. Le PL64 devrait donner à l'entreprise le choix du processus qui lui convient le mieux en fonction de ses opérations pour procurer au consommateur une meilleure protection.

De plus, l'évaluation devrait être requise uniquement en fonction de la nature des renseignements recueillis et lorsqu'un seuil de matérialité est atteint. D'ailleurs, le RGPD prévoit à l'article 35 un seuil de matérialité en indiquant qu'une analyse d'impact relative à la protection des données est nécessaire : « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Le BAC recommande de modifier l'article 3.3 alinéa 1 comme suit :

Toute personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée lorsqu'un projet de système d'information ou de prestation électronique de services implique la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Cette évaluation est requise uniquement si la sensibilité des renseignements personnels et la finalité de leur utilisation sont susceptibles de créer un risque réel de préjudice sérieux.

Article 3.4

Le BAC recommande le retrait de cet article. Cet article est trop prescriptif dans la mesure où il indique que c'est le responsable de la protection des renseignements personnels qui doit intervenir. Comme mentionné précédemment, il est important de permettre à une entreprise d'établir sa gouvernance en toute flexibilité. Une entreprise pourrait ainsi déterminer que ces tâches reviennent à d'autres employés. Encore ici, de telles précisions nous paraissent très techniques et spécifiques et devraient relever de la gestion interne d'une entreprise qui doit pouvoir établir elle-même ses règles de gouvernance en fonction de son modèle d'affaires.

Article 3.5

L'article 3.5 exige le signalement des incidents de confidentialité lorsqu'un risque réel de préjudice sérieux est présent. Bien que le seuil pour signaler un incident soit semblable à celui qui se retrouve dans la LPRPDE et le RGPD, les exigences pour la divulgation sont différentes et créent de l'incertitude. La portée d'un incident de confidentialité impliquant une entreprise québécoise s'étend souvent à d'autres provinces canadiennes ou à l'étranger. D'ailleurs, les incidents de confidentialité qui ont fait les manchettes dans les dernières années n'étaient pas limités aux résidents québécois. Les entreprises québécoises peuvent être tenues de respecter les lois de diverses juridictions quant à la divulgation des incidents de confidentialité. Or, si le processus de divulgation diffère trop d'une juridiction à une autre, cela engendrera des difficultés d'application et des situations incohérentes.

Par exemple, en vertu de l'article 10.1 (3) de la LPRPDE, une entreprise est tenue de divulguer l'incident à un individu concerné, sauf si une règle de droit l'interdit, alors que l'article 3.5 alinéa 3 du PL64 indique que l'entreprise n'a pas à procéder à une telle divulgation si elle est susceptible de nuire à une enquête. Donc, si un incident de confidentialité implique des résidents du Québec et de l'Ontario, l'entreprise pourrait être tenue de divulguer l'incident de confidentialité aux individus résidant en Ontario, mais pas à ceux résidant au Québec, puisque les exigences quant au signalement diffèrent.

Cette nouvelle exigence relative aux enquêtes est difficile d'application et crée de l'incertitude pour les entreprises qui souhaitent divulguer l'incident à l'individu concerné en temps utile pour en minimiser les conséquences, car la Loi ne précise pas dans quel contexte exactement l'entreprise n'est pas tenue de divulguer l'incident. Or, les conséquences de l'inaction de cette dernière pourraient être importantes et entraîner sa responsabilité envers l'individu concerné. Aussi, à moins d'être avisée par la personne ou l'organisme chargé de mener l'enquête, l'entreprise ne détiendra pas les informations nécessaires pour déterminer si la divulgation pourrait nuire à cette enquête. Le BAC est d'avis que les critères de divulgation doivent être précis et limitatifs afin d'éviter toute subjectivité dans l'application de cet article. C'est d'ailleurs cette approche qu'a retenue le législateur fédéral en indiquant à l'article 10.1 (3) de la LPRPDE que l'organisation est tenue d'aviser l'individu concerné à moins qu'une règle de droit l'interdise**. Le BAC recommande donc d'harmoniser les critères de divulgation d'un incident de confidentialité avec la LPRPDE**. **Si le législateur souhaite créer une exception en ce qui concerne les enquêtes, le BAC recommande d'indiquer clairement et limitativement les modalités de cette obligation**.

L'article 3.5 alinéa 2 précise que si l'incident de confidentialité présente un risque de préjudice sérieux, l'entreprise peut aviser d'autres organismes susceptibles de réduire le risque et que dans ce cas, l'entreprise doit enregistrer la communication. Cette obligation nous apparaît trop prescriptive. **Le BAC recommande d'adopter une approche davantage basée sur les principes, en modifiant le terme « enregistrer » par « documenter »**.

Finalement, les assureurs sont tenus en vertu de la *Ligne directrice sur la gestion du risque opérationnel*[7] de divulguer les incidents opérationnels majeurs à l'Autorité, ce qui inclut les incidents de confidentialité. La *Ligne directrice sur les saines pratiques commerciales*[8] indique également que l'assureur doit notifier l'Autorité de tout incident de confidentialité susceptible de nuire aux intérêts des consommateurs. Pour éviter que les assureurs soient tenus à des instructions contradictoires, **le BAC recommande de préciser que les assureurs devront suivre les instructions de l'Autorité ou de leur régulateur pour la gestion des incidents de confidentialité**.

Le BAC recommande :

- D'harmoniser les règles de divulgation d'un incident de confidentialité avec celles prévues à la LPRPDE;
- De modifier la dernière phrase de l'article 3.5 alinéa 2 afin qu'elle se lise comme suit :

  « Dans ce dernier cas, l'entreprise doit documenter la communication »;
- Harmoniser l'article 3.5 alinéa 3 avec l'article 10.1 (3) de la LPRPDE, et si le législateur souhaite créer une exception, remplacer l'article 3.5 alinéa 3 par ce qui suit :

[7] P. 11.
[8] P. 20.

« Malgré le deuxième alinéa, si une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois informe la personne qui exploite une entreprise que la divulgation est susceptible d'entraver une enquête, cette dernière n'est pas tenue d'aviser la personne concernée. »;

- Préciser qu'à la suite d'un incident de confidentialité, les assureurs devront suivre en priorité les instructions de l'Autorité ou de leur régulateur pour la gestion des incidents de confidentialité.

Article 3.6

La LPRPDE et le RGPD limitent le signalement aux trois situations suivantes : un accès non autorisé, une divulgation (communication) non autorisée ou une perte de renseignements personnels. Au Québec, le législateur propose à l'article 3.6 une quatrième situation qui constitue un incident de confidentialité nécessitant une divulgation, soit l'utilisation non autorisée. Cette exigence additionnelle au Québec crée une difficulté d'application pour les entreprises, car celles-ci ne pourront pas toujours savoir si l'utilisation des renseignements découle de l'accès non autorisé, de la communication non autorisée ou de la perte survenue précédemment. L'utilisation des renseignements personnels, qui survient après l'accès, la communication ou la perte, est plutôt une conséquence de l'incident de confidentialité sur laquelle l'entreprise n'a généralement pas le contrôle. Le BAC est donc d'avis que l'utilisation ne devrait pas être définie comme un incident de confidentialité sujet à la divulgation par l'entreprise au même titre que l'accès, la communication ou la perte.

Le paragraphe 4 de l'article 3.6 précise qu'un incident de confidentialité comprend « toute autre atteinte à la protection d'un tel renseignement ». Cette définition est beaucoup trop large et imprécise. Considérant les importantes sanctions et pénalités auxquelles font face les entreprises qui ne divulguent pas un incident de confidentialité, il est primordial que la définition d'incident ne soit pas ambiguë quant aux obligations des parties.

Le BAC recommande donc :

- **D'harmoniser la définition d'incident de confidentialité avec la LPRPDE et le RGPD en retirant le 2e paragraphe de l'article 3.6 du PL64 qui se lit comme suit : « 2° L'utilisation non autorisée par la loi d'un renseignement personnel. »**
- **Retirer au paragraphe 4 de l'article 3.6 « ou toute autre atteinte à la protection d'un tel renseignement ».**

Article 3.7

L'article 3.7 précise que, lors de l'évaluation d'un incident de confidentialité, le responsable de la protection des renseignements personnels doit être consulté. Cette exigence, qui est de nature opérationnelle, limite inutilement l'entreprise en ce qui concerne sa gouvernance. La Loi devrait préciser les résultats attendus et s'abstenir de préciser les moyens pour y arriver.

De plus, l'évaluation prévue à l'article 3.7 a pour but de déterminer si l'incident peut causer un préjudice sérieux à la personne concernée. Le terme « sérieux » devrait donc être ajouté après « préjudice », ce qui permettrait une harmonisation terminologique avec l'expression utilisée à l'article 3.5.

Le BAC recommande :

- **D'ajouter le terme « sérieux » à la suite de « préjudice » à la première phrase de l'article;**
- **Le retrait de la dernière phrase de l'article 3.7.**

Article 3.8

Le BAC recommande que le règlement qui précisera la teneur du registre s'harmonise avec les autres lois pour éviter qu'une entreprise doive maintenir plusieurs registres ayant un objectif semblable.

SECTION II
COLLECTE DE RENSEIGNEMENTS PERSONNELS

Article 8

L'article 8 du PL64 ajoute des informations à divulguer à la personne concernée et introduit le fait que certaines informations devront être divulguées lors de la collecte. Ces nouvelles obligations apparaissent difficilement conciliables avec la réalité des représentants qui offrent des services au téléphone et semblent prendre en considération uniquement un modèle d'affaires en ligne. En effet, les modèles d'affaires par internet permettent de regrouper ces informations dans un document explicatif à l'intention des consommateurs, disponible avant, pendant et après la collecte, alors qu'il est impensable de donner l'ensemble de ces informations à l'occasion d'un appel avec le client.

Le BAC est d'avis que plusieurs de ces informations ne sont pas pertinentes au moment de la collecte pour que le consommateur puisse donner un consentement libre et éclairé. C'est le cas par exemple du droit d'accès et de rectification prévu à la Loi. Cette information devient pertinente uniquement lorsque le consommateur souhaite savoir comment accéder à son dossier.

De plus, le fait de recevoir beaucoup d'informations lors de la collecte ne favorise pas l'obtention du consentement libre et éclairé. Au contraire, une avalanche d'informations a pour effet de diluer l'information pertinente à la prise de décision et de nuire à la bonne compréhension des éléments clés menant à un consentement éclairé. Par exemple, on peut penser aux consommateurs qui cliquent sur « Oui, j'ai compris » alors qu'ils n'ont pas lu le texte de consentement relativement aux fichiers témoins (« *cookies* ») placés par l'entreprise sur un site internet. Nous sommes à une époque où les consommateurs veulent trouver et obtenir l'information qu'ils recherchent rapidement. Donc, en plus de potentiellement miner son consentement éclairé, donner une multitude d'informations au consommateur pourrait le pousser à abandonner son processus d'achat d'assurance.

Le paragraphe 4 du premier alinéa de l'article 8 précise que l'entreprise doit informer le consommateur de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis. Or, il faut comprendre que dans certains cas, le retrait du consentement à l'utilisation des renseignements entraîne la cessation des services par l'entreprise. Par exemple, lorsque le client adhère à un programme de télématique, les données recueillies en temps réel sont nécessaires, car elles permettent d'établir la prime en fonction du comportement de conduite de l'assuré. Le retrait du consentement quant à l'utilisation des renseignements divulgués par les clients pourrait même empêcher l'assureur de lui offrir des

produits d'assurance puisque ceux-ci sont utilisés notamment à des fins de souscription et de tarification.

L'alinéa 3 de l'article 8 précise que l'entreprise doit, sur demande, informer le consommateur des renseignements personnels recueillis auprès de lui, des catégories de personnes au sein de l'entreprise qui ont accès à ses renseignements et de la durée de conservation de ces renseignements. Le BAC considère que cette information n'a pas de valeur ajoutée pour le consommateur et recommande de la retirer.

Le BAC recommande de :

- Modifier l'alinéa 1 de l'article 8 afin de limiter les renseignements à divulguer à ceux pertinents au moment de la collecte, soit ceux prévus aux paragraphes 1 et 2. Autoriser l'entreprise à diriger la personne concernée vers la politique sur les renseignements personnels publiés sur le site internet de l'entreprise ou lui indiquer qu'elle est disponible sur demande pour obtenir plus de précisions concernant la protection des renseignements personnels;
- Modifier l'alinéa 3 de l'article 8 afin de retirer l'obligation d'informer le consommateur des renseignements personnels recueillis auprès de lui et des catégories de personnes au sein de l'entreprise qui ont accès à ses renseignements ou de maintenir le statu quo en conservant les obligations prévues dans la *Loi sur le secteur privé*.

Article 8.1

Le paragraphe 2 de l'alinéa 1 de l'article 8.1 exige d'informer le consommateur des moyens offerts pour désactiver les fonctions permettant de l'identifier, de le localiser ou d'effectuer un profilage. Le BAC souligne que les représentants en assurance ne sont pas des experts en technologie et ne sont pas toujours qualifiés pour expliquer au client comment désactiver le système, et ce d'autant plus qu'il existe plusieurs variétés de systèmes, ce qui ne permet pas une connaissance généralisée.

Aussi, il ne paraît pas opportun de permettre la désactivation de certains systèmes si les données de profilage sont essentielles pour offrir le produit ou le service. En effet, les assureurs ont développé, par l'entremise des nouvelles technologies, des produits et services au bénéfice des consommateurs. Tel est notamment le cas de la télématique, qui a pour objectif d'établir le plus précisément possible le profil de risque de l'assuré en analysant son comportement au volant. Les données de conduite recueillies technologiquement sont donc essentielles pour offrir le produit.

Le BAC recommande donc que l'obligation prévue au paragraphe 2 du premier alinéa de l'article 8.1 ne soit pas impérativement exécutée au moment de la cueillette par la personne responsable de cette tâche, mais sur demande par tout moyen approprié.

Article 8.2

L'article 8.2 exige de publier la politique de confidentialité et des modifications subséquentes à celle-ci sur le site internet de l'entreprise et de la diffuser par tout moyen propre à atteindre les personnes concernées.

L'obligation de publier la politique de confidentialité est déjà prévue à l'article 3.2 du PL64. **Pour éviter toute confusion, le BAC recommande de maintenir uniquement l'obligation prévue à l'article 3.2.**

Quant à l'obligation de diffuser la politique et les avis de modification, le BAC recommande de limiter cette obligation à indiquer clairement que la politique a été modifiée.

Article 9.1

L'article 9.1 exige que, par défaut, les paramètres de produits ou services technologiques assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée. Cette règle est similaire à celle retrouvée à l'article 25 du RGPD quant à la protection des renseignements personnels dès la conception (*privacy by default*). Cette notion européenne a d'ailleurs fait l'objet d'une consultation récente[9].

Or, l'article 9.1 du PL64 n'intègre aucune notion de proportionnalité comme le fait l'article 25 du RGPD, qui prévoit une modulation de cette obligation en fonction de plusieurs critères, tels que l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités des renseignements personnels, ainsi que des risques, dont le degré de probabilité et de gravité.

Le BAC recommande d'introduire à l'article 9.1 des critères semblables à ceux du RGPD.

SECTION III
CARACTÈRE CONFIDENTIEL DES RENSEIGNEMENTS PERSONNELS

§ 1. — DÉTENTION, UTILISATION ET NON COMMUNICATION DES RENSEIGNEMENTS

Article 12

Le consentement est un élément central de la *Loi sur le secteur privé*. Or, les précisions apportées par le PL64 quant au type de consentement requis créent de la confusion, car l'article tel que rédigé exige une lecture à *contrario* pour déterminer que le consentement implicite est permis. Considérant les sanctions auxquelles une entreprise peut être soumise en cas d'erreur ou d'incompréhension sur le type de consentement requis pour l'utilisation des renseignements personnels, le BAC souhaite que l'article 12 du PL64 soit précisé pour éviter différentes interprétations.

De plus, le BAC est d'avis que le consentement implicite devrait s'appliquer tant pour les fins pour lesquelles il a été recueilli que pour toutes autres fins, pourvu que les critères prévus pour satisfaire à l'obligation de transparence de l'article 14 soient respectés. Le BAC réitère que la qualité du consentement devrait dépendre des circonstances, notamment de la sensibilité des renseignements recueillis. C'est d'ailleurs l'approche qui a été retenue par le législateur fédéral, qui permet un consentement explicite ou implicite selon les circonstances, les types de renseignements et les attentes raisonnables de la personne concernée. Quant au RGPD, le consentement explicite est uniquement nécessaire pour le traitement de certains renseignements personnels.

Le BAC recommande donc de permettre clairement le consentement implicite pour les utilisations primaires et secondaires, mais en précisant que le consentement pourra

[9] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adopté le 13 novembre 2019, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

varier selon les circonstances et la nature des renseignements collectés. Ceci permettrait une flexibilité pour les entreprises et une harmonisation avec l'article 4.3.6 de l'Annexe I de la LPRPDE.

L'utilisation des renseignements pour créer des modèles actuariels est primordiale pour les assureurs. L'analyse des données actuarielles permet entre autres d'établir la prime en regard du risque souscrit. Elle permet également à l'entreprise d'établir son portefeuille de risques en respect des règles de gouvernance édictées par les lois sectorielles et par les lignes directrices de l'Autorité des marchés financiers. Il est dans l'intérêt des consommateurs que les compagnies d'assurance puissent continuer à utiliser les renseignements personnels pour innover, améliorer l'expérience client et réduire les coûts associés à l'assurance. **Le BAC comprend que l'utilisation des données à des fins actuarielles est une fin compatible avec celles pour lesquelles les renseignements ont été recueillis, conformément à l'article 12 alinéa 2 paragraphe 1. Si la compréhension du BAC n'est pas exacte, une exception distincte pour les activités actuarielles des assureurs doit être prévue à cet effet.**

Le troisième alinéa de l'article 12 interdit d'utiliser les renseignements personnels à des fins secondaires sans le consentement de la personne concernée lorsqu'il s'agit de prospection commerciale. Or, plusieurs produits peuvent venir compléter ou bonifier une couverture d'assurance au bénéfice de l'assuré. D'ailleurs, en vertu de l'article 27 de la *Loi sur la distribution de produits et services financiers*, un représentant en assurance est dans l'obligation d'offrir les produits d'assurance qui conviennent le mieux aux besoins du client. Il est donc inapproprié de réduire l'offre d'assurance par un représentant certifié en imposant un fardeau administratif tel que l'obtention d'un nouveau consentement sous prétexte qu'il ne s'agit pas d'une fin compatible avec l'utilisation principale.

Les assureurs doivent avoir la possibilité de continuer de communiquer à leurs clients des informations concernant des produits pouvant répondre à leurs besoins. À cet égard, il est important d'apporter une distinction entre de la prospection commerciale effectuée par une entreprise tierce à la suite de la vente d'une liste nominative, par exemple, et la prospection commerciale effectuée par l'assureur ou une institution de son groupe. Le BAC est d'avis que cette utilisation au sein d'un même groupe est complémentaire et bénéfique. Le BAC recommande le retrait de l'alinéa 3 de l'article 12 ou l'ajout d'une exception afin de prendre en considérations les attentes des assurés et les particularités de l'assurance de dommages.

Le BAC recommande les modifications suivantes :

- Harmoniser l'alinéa 1 de l'article 12 avec l'article 4.3.6. de l'Annexe 1 de la LPRPDE;
- Si nécessaire, prévoir une exception distincte pour que l'utilisation des données à des fins actuarielles par les assureurs soit considérée comme une fin compatible avec celles pour lesquelles les renseignements ont été recueillis;
- Retirer la dernière phrase de l'alinéa 3 qui se lit comme suit :
  « Toutefois, ne peut être considérée comme une fin compatible la prospection commerciale ou philanthropique. » ou ajouter une exception afin de prendre en considération les particularités de l'assurance de dommages.

Article 12.1

Lorsqu'une décision est fondée exclusivement sur un traitement automatisé, l'article 12.1 du PL64 octroie aux personnes concernées le droit de recevoir certaines informations et de fournir ses observations à un membre du personnel en mesure de réviser la décision. Ce nouveau droit semble inspiré du droit d'opposition prévu à l'article 21 du RGPD. Toutefois, l'article 12.1 vise

tous les types de traitements automatisés sans distinction, contrairement à l'article 21 du RGPD qui prévoit un droit d'opposition absolu uniquement lorsque le traitement automatisé est utilisé à des fins de prospections commerciales. Les articles 21 et 22 du RGPD prévoient également de nombreuses et importantes exceptions et conditions à ce droit, par exemple lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et une entreprise. Les droits prévus à l'article 12.1 posent principalement deux difficultés.

Premièrement, les informations à fournir, dont celles prévues au paragraphe 2 du deuxième alinéa de l'article 12.1, pourraient entraîner la divulgation de secrets commerciaux, tels que la stratégie d'affaires, et affecter la concurrence. Les exceptions prévues au RGPD permettent de prévenir une telle situation. Par exemple, le mécanisme pour établir les primes d'assurance constitue une information confidentielle très sensible pour les assureurs et pas nécessairement pertinente pour un consommateur. De plus, l'offre d'assurance en ligne est déjà encadrée par le *Règlement sur les modes alternatifs de distribution*[10] qui précise les renseignements que l'assureur doit fournir avant, pendant et sur demande à l'assuré afin qu'il puisse prendre une décision libre et éclairée. **Le BAC est d'avis que l'article 12.1 alinéa 2 devrait être modifié afin d'y inclure des exceptions semblables à celles qui se retrouvent aux articles 21 et 22 du RGPD.**

Deuxièmement, le droit de fournir ses observations pour tout traitement automatisé sans exception est un fardeau administratif important pour les entreprises. Le BAC est d'avis qu'il est important que l'ensemble des processus d'affaires, incluant le traitement informatisé, demeurent une prérogative des entreprises dans la mesure où ces processus sont raisonnables et respectent les lois applicables. Les assureurs sont encadrés par la *Loi sur les assureurs* et la *Ligne directrice sur les saines pratiques commerciales* de l'Autorité en ce qui a trait au traitement équitable des consommateurs. Ainsi, il est déjà prévu que les demandes des assurés, incluant les plaintes, doivent être traitées avec diligence et de façon équitable par les assureurs. **Le BAC est d'avis que l'encadrement actuel des assureurs est suffisant pour protéger le consommateur et recommande de retirer l'article 12.1 alinéa 3.**

Le BAC recommande de :

- Modifier l'article 12.1 alinéa 2 afin d'y inclure des exceptions semblables à celles qui se retrouvent aux articles 21 et 22 du RGPD ;
- Retirer l'article 12.1 alinéa 3.

Article 13

Comme précisé plus haut à l'égard de l'article 12, le consentement explicite ne devrait pas être automatiquement exigé pour les renseignements sensibles. Le BAC reconnaît l'importance de prendre en considération la sensibilité des renseignements afin de déterminer quel type de consentement est approprié, mais ce consentement devrait varier selon les circonstances et la nature des renseignements collectés. **Le BAC recommande de modifier le deuxième alinéa de l'article 13 comme suit :**

« L'entreprise doit prendre en considération la nature des renseignements collectés et les circonstances de cette collecte pour déterminer si celui-ci doit être manifesté de façon expresse. »

[10] RLRQ c. D-9.2, r.15.1, http://canlii.ca/t/6cbn3

Article 14

L'article 14 prévoit que le consentement doit être donné à des fins spécifiques, distinctement de toute autre information communiquée à la personne concernée. Or, le PL64 permet aux entreprises d'obtenir un consentement implicite ou explicite selon les circonstances applicables. **À cet égard, le BAC recommande d'apporter la précision suivante à l'article 14 alinéa 1:**

> « Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. **Lorsqu'un consentement explicite est requis**, il est demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé ».

Le BAC recommande également de préciser dans les dispositions transitoires que les consentements obtenus et les listes nominatives créées avant l'entrée en vigueur des modifications demeurent valides.

Article 17

L'article 17 permet le transfert de renseignements personnels à l'extérieur du Québec uniquement si l'évaluation des facteurs relatifs à la vie privée détermine que les renseignements bénéficieraient d'une protection équivalente à celle prévue par la Loi. Cette nouvelle exigence est dérivée des règles prévues par le RGPD. Toutefois, ce dernier règlement permet le transfert à travers les pays de l'Union européenne (UE) et ne crée pas de barrière inutile entre juridictions. Plusieurs entreprises québécoises ont des bureaux dans le reste du Canada et conservent leurs données à l'extérieur du Québec. Considérant que le Canada est un partenaire commercial important pour le Québec, il est primordial d'assurer la stabilité des ententes commerciales en place et d'alléger le fardeau de conformité des entreprises exerçant leurs activités à travers le Canada en leur offrant un cadre législatif sans barrière artificielle. **Le BAC recommande donc que l'article 17 vise uniquement les transferts à l'extérieur du Canada.**

De plus, le 1er juillet dernier, l'*Accord entre le Canada, les États-Unis d'Amérique et les États-Unis Mexicains*[11] entrait en vigueur. L'article 19.8 de cet Accord prévoit des règles concernant la protection des renseignements personnels, y compris sur le transfert transfrontalier des renseignements entre ces pays. L'article 19.8 paragraphe 6 précise que les États peuvent adopter des approches juridiques différentes, mais devraient s'efforcer d'encourager l'élaboration de mécanismes favorisant une compatibilité entre les différents régimes. Également, l'article 19.8 paragraphe 3 précise que les restrictions des échanges transfrontières de renseignements personnels doivent être nécessaires et demeurer proportionnelles aux risques associés. **Le BAC recommande donc l'intégration d'un mécanisme spécifique pour le transfert aux États-Unis qui permettrait de respecter les objectifs de l'Accord.**

L'évaluation des facteurs relatifs à la vie privée tel que prévu au PL64 constitue un processus administratif très lourd et très coûteux. Par exemple, le 4e paragraphe du premier alinéa de l'article 17 indique que l'entreprise doit évaluer si le régime juridique de l'État où les renseignements seront communiqués est équivalent à celui du Québec, ceci dans tous les cas

[11] Accord entre les États-Unis d'Amérique, les États-Unis Mexicains et le Canada, https://www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/r-aceum-00.pdf

où l'État ne sera pas listé à l'article 17.1. Or, seuls des juristes spécialisés dans cet État peuvent effectuer une telle analyse.

Le BAC s'inquiète également de la possibilité qu'un État reconnu comme équivalent par l'article 17.1 soit retiré de la liste. Or, ce retrait pourrait avoir des conséquences importantes sur les entreprises qui ont contracté avec des entreprises de ces juridictions. Le PL64 doit prévoir qu'une entreprise qui contracte avec une entreprise d'une autre juridiction ayant une équivalence juridique au moment où le contrat entre en vigueur ne contrevient pas à la Loi tant et aussi longtemps que la relation contractuelle n'est pas terminée.

Pour les mêmes raisons, les dispositions transitoires du PL64 doivent prévoir des mesures de sauvegarde pour les entreprises qui ont des contrats en vigueur avec des entreprises basées dans d'autres juridictions, avant l'entrée en vigueur de la Loi afin de ne pas être dans l'obligation de mettre fin au contrat. **Le BAC recommande donc que les dispositions transitoires contiennent un droit acquis pour les entreprises qui ont des contrats en vigueur dans d'autres juridictions que le Canada.**

Aussi, le BAC recommande que l'article 17 permette d'autres mécanismes que le test de « protection équivalente à celle prévue par la loi » pour le transfert à l'extérieur du Canada. L'article 17 devrait permettre aux entreprises de transférer des renseignements personnels dans une autre juridiction dans la mesure où des garanties appropriées sont obtenues. Par exemple, une approche basée sur le principe de responsabilité, qui rend l'entreprise imputable des actions de ses fournisseurs de services, permettrait une protection robuste des renseignements personnels tout en offrant une certaine souplesse. D'ailleurs, l'article 46 du RGPD prévoit cette option. Selon la Commission européenne (CE), l'utilisation des *clauses contractuelles types*[12] constitue l'outil de transfert de renseignements personnels le plus couramment utilisé.

Finalement, le PL64 devrait prévoir des exceptions à l'article 17 pour des situations particulières. À cet égard, l'article 49 du RGPD prévoit une liste de dérogations, notamment lorsque la personne concernée donne son consentement, lorsque le transfert est nécessaire à la conclusion d'un contrat conclu dans l'intérêt de la personne concernée et lorsque le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice. Les assureurs offrent des produits d'assurance responsabilité avec une protection mondiale à leurs assurés. Ainsi, si un assuré fait l'objet d'une poursuite dans une juridiction qui n'a pas une protection équivalente en matière de protection de renseignements personnels, l'assureur est tout de même tenu d'entreprendre des démarches pour protéger et sauvegarder les droits de son assuré. Ces démarches peuvent impliquer des transferts d'informations. Il importe que les assureurs puissent continuer à remplir leurs obligations à l'égard de leurs clients et leur procurer le support auquel ils ont droit, particulièrement dans le type de situation ci-haut mentionné qui peut être une source de préoccupations importante pour eux.

Le BAC recommande donc les modifications suivantes aux articles 17 et 17.1 concernant le transfert de données :

- Modifier la première phrase de l'article 17 comme suit :

[12] «Ces clauses constituent, de loin, le mécanisme le plus largement utilisé pour les transferts de données; des milliers d'entreprises de l'UE y ont recours pour fournir un large éventail de services à leurs clients, fournisseurs, partenaires et employés», *Communication de la Commission au parlement européen et au Conseil, La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données*, p 13. Commission Européenne, 24 juin 2020.

« Avant de communiquer à l'extérieur du Canada un renseignement personnel, la personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée. »;

- Inclure dans les dispositions transitoires du PL64 des droits pour les entreprises qui ont contracté avec d'autres entreprises dans des juridictions qui ne figurent pas sur la liste du gouvernement à l'entrée en vigueur de la Loi;
- Ajouter d'autres mécanismes de protection à celui de la protection équivalente comme mécanismes contractuels comportant des garanties suffisantes;
- Ajouter des exceptions à l'article 17 pour des situations particulières afin de permettre le transfert de renseignements personnels, notamment pour protéger les droits d'une personne concernée;
- Modifier l'article 17.1 afin qu'il prévoie que si un État est retiré de la liste, les entreprises qui ont des contrats en vigueur avec des entreprises de ces juridictions peuvent continuer à faire affaire avec celles-ci jusqu'à l'expiration du contrat sans contrevenir à la Loi.

§ 2. — COMMUNICATION À DES TIERS

Article 18

L'article 18 prévoit que les entreprises peuvent communiquer des renseignements personnels sans le consentement de la personne concernée dans certaines situations. Le 3e paragraphe du premier alinéa de l'article 18 permet une telle communication à un organisme chargé de prévenir, détecter ou réprimer les crimes. Cet article permet également aux entreprises de communiquer des renseignements personnels à une autre entreprise si elle a des motifs raisonnables de croire que la personne concernée a commis ou est sur le point de commettre un crime à son égard. On vise uniquement des situations où la fraude est imminente, limitant ainsi la collaboration entre les assureurs pour prévenir la fraude de façon plus globale.

L'industrie de l'assurance est particulièrement concernée par la fraude. Il s'agit d'un crime qui génère de graves conséquences pour tous les assurés notamment en affectant leur prime. D'ailleurs, les experts en sécurité reconnaissent une valeur inhérente au partage de l'information pour combattre la fraude et la cybercriminalité. La prévention doit être au cœur de la stratégie antifraude pour maximiser son efficience.

Depuis plusieurs années, le BAC collabore avec les autorités chargées de prévenir, détecter ou réprimer le crime pour contrer ce fléau. Cette collaboration est facilitée notamment par la création d'exceptions dans la loi pour faciliter l'échange de renseignements personnels. En 2015, la LPRPDE a introduit les articles 7 (3) d.1 et 7 (3) d.2 qui autorisent la communication entre organisations sans le consentement de la personne concernée, en vue de la prévention, de la détection ou de la suppression de la fraude. Malheureusement, ces dispositions se limitent également à permettre la communication de renseignements lorsque la fraude est imminente, sans préciser qu'un assureur peut collecter et utiliser des renseignements personnels pour prévenir la fraude. Cette approche crée beaucoup d'incertitude dans l'industrie et affecte l'efficacité des mesures antifraude. Les fraudeurs sont en mesure de faire preuve de beaucoup de créativité pour perpétrer leurs forfaits. Or, malheureusement, le libellé du PL64 en la matière est de nature à restreindre sérieusement les démarches légitimes des assureurs pour contrer les fraudeurs, et ce, au détriment de tous les assurés québécois.

À cet égard, le régime législatif[13] en Grande-Bretagne autorise plus largement la communication, le partage et l'utilisation pour la prévention de la fraude, qui est considérée comme un « intérêt légitime ».

Le BAC recommande donc de modifier le 3e paragraphe du premier alinéa de l'article 18 afin de permettre aux assureurs de collecter, d'utiliser ou d'échanger des renseignements avec un autre organisme ou une autre entreprise afin de prévenir, détecter ou supprimer la fraude et que l'obtention du consentement de la personne concernée ne puisse être obtenu sans compromettre la réalisation de cet objectif.

Article 18.3

L'article 18.3 prévoit qu'une entreprise qui impartit des services à des tiers peut lui transférer des renseignements personnels sans le consentement de la personne concernée sous réserve de prévoir contractuellement les mesures à prendre quant à ces renseignements. Considérant que les contrats de ce type peuvent être en vigueur pour encore un certain nombre d'années, il est important de préciser dans les dispositions transitoires que ceux-ci bénéficieront d'un droit acquis jusqu'à leur expiration.

Par ailleurs, le BAC est d'avis que les organismes publics ne devraient pas être exclus de l'application du 2e paragraphe du deuxième alinéa de l'article 18.3 lorsqu'ils sont mandataires ou exécutants du contrat. En effet, il est important que l'organisme public avise sans délai l'entreprise en cas d'incident de confidentialité afin qu'elle puisse prendre les mesures de protection nécessaires pour sécuriser les renseignements et aviser la personne concernée de cet incident. Autrement, l'entreprise pourra être tenue responsable par la personne concernée. **Le BAC recommande de retirer le 3e alinéa de l'article 18.3.**

Article 18.4

Le BAC salue cette nouvelle exception qui est importante pour les entreprises. **Par ailleurs, le BAC recommande d'harmoniser l'article 18.4 avec l'article 7.2 de la LPRPDE en modifiant la définition de transaction commerciale prévue à l'alinéa 4 de l'article 18.4**. En effet, cette définition est limitée à un transfert de propriété, en tout ou partie, d'une entreprise, tandis que la définition de la loi fédérale vise également la fusion, les transactions financières comme le fait de consentir un prêt à une entreprise ou de lui fournir toute autre forme de financement ou la location d'éléments d'actifs d'une entreprise ou d'une licence à cet égard.

Article 22

Le PL64 élimine l'exception concernant les listes nominatives qui est prévue à l'article 22 de la *Loi sur le secteur privé* actuelle. Or, cette pratique est actuellement bien encadrée et la personne concernée détient un droit de refuser que ses informations soient utilisées par un tiers à des fins de prospection commerciale. Cette exception a également permis à l'industrie de développer des partenariats et des groupes d'affinités auprès d'organismes et d'entreprises qui bénéficient de ces offres, en obtenant des renseignements sur des produits d'assurances ou financiers complémentaires de l'assureur ou des institutions financières qui composent son groupe financier.

[13] *Data Protection Act, 2018 UK Public General Acts, 2018 c.12 et* le *Serious Crime Act, 2007*, *UK Public General Acts, 2018 c.12,* articles 68 à 72.

Il n'a jamais été porté à la connaissance de l'industrie de l'assurance que cette pratique constituait un enjeu. D'ailleurs, le *Rapport quinquennal de la CAI*[14] ne fait pas mention de cet article ni d'aucune problématique occasionnée par les listes nominatives et la prospection commerciale. De plus, les assureurs doivent maintenir un registre de plainte conformément à la *Loi sur les assureurs*[15] et les plaintes concernant les listes nominatives n'ont jamais été identifiées comme un problème par l'industrie de l'assurance. **Le BAC recommande donc de conserver l'article 22 de la *Loi sur le secteur privé* actuelle. Alternativement, si cette exception n'est pas conservée, prévoir une exception pour les entreprises qui forment un groupe financier.**

Si l'article 22 du PL64 est maintenu, les entreprises doivent avoir un délai pour se conformer à l'obligation de retirer le consentement de la personne concernée. Une entreprise devrait bénéficier d'un délai d'au moins 10 jours pour retirer la personne de la liste. D'ailleurs, la *Loi canadienne anti-pourriel*[16] prévoit à l'article 11 (3) un délai de 10 jours ouvrables pour retirer d'une liste de sollicitation une personne qui reçoit un message électronique commercial.

Il sera également important de prévoir aux dispositions transitoires un droit acquis pour les listes nominatives créées avant l'entrée en vigueur des nouvelles dispositions.

§ 3. — DESTRUCTION OU ANONYMISATION

Article 23

L'article 23 prévoit la destruction ou l'anonymisation des renseignements personnels lorsque les fins auxquelles un renseignement personnel a été recueilli ont été accomplies. L'anonymisation des renseignements personnels est un processus laborieux et exigeant au niveau technique. De plus, l'anonymisation s'applique difficilement dans le contexte de l'assurance, et ce, pour deux raisons : 1) une réclamation peut se déclencher bien après la date d'expiration de la police, en responsabilité civile par exemple, et si les données sont anonymisées, l'assureur ne pourra pas exécuter ses obligations contractuelles; 2) afin d'accomplir leur mission, les assureurs doivent créer des modèles de tarification basés sur le plus de données possible. Ces modèles incluent, par exemple, l'adresse qui permet indirectement de trouver le nom du propriétaire d'un bâtiment. Conséquemment, forcer les assureurs à anonymiser les renseignements mettrait en péril la modélisation nécessaire pour établir la tarification et le respect des exigences législatives. **Conséquemment, le BAC recommande d'ajouter l'option de *dépersonnaliser* à l'article 23 (1) qui devrait être modifié comme suit :**

> **« Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire, le dépersonnaliser ou l'anonymiser, sous réserve d'un délai de conservation prévu par une loi ».**

---

[14] Commission d'accès à l'information, *Rétablir l'équilibre, Rapport quinquennal* 2016, https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf

[15] *Loi sur les assureurs*, A-31.1.

[16] Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la *Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes*, la *Loi sur la concurrence*, la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur les télécommunications*, L.C. 2010, ch. 23.

De plus, l'obligation de détruire, de dépersonnaliser ou d'anonymiser devrait s'appliquer uniquement aux renseignements personnels collectés après l'entrée en vigueur du PL64 afin d'éviter des modifications très importantes et très onéreuses aux systèmes existants (*legacy system*). **À cet égard, le BAC recommande que les dispositions transitoires prévoient un droit acquis pour ces renseignements**.

Le BAC recommande de retirer l'alinéa 3 de l'article 23 du PL64. Il est curieux de préciser que les meilleures pratiques doivent être utilisées pour l'anonymisation dans la mesure où les entreprises ont déjà l'obligation de prendre les mesures de sécurité propres à assurer la protection des renseignements conservés ou détruits en vertu de l'article 10. Cet ajout dans la section « Destruction et anonymisation » engendrera fort probablement de la confusion entre ces deux obligations. Par ailleurs, le BAC se questionne sur ce qu'on désigne réellement par « meilleures pratiques ». Celles-ci peuvent varier en fonction de la taille et du champ d'opération des entreprises. En effet, une « meilleure pratique » pour un géant du web ne devrait pas être applicable à une petite entreprise. Le libellé du PL64 devrait tenir compte du contexte dans lequel les entreprises font affaire et de leur taille.

SECTION IV
ACCÈS DES PERSONNES CONCERNÉES

§ 1. — DISPOSITIONS GÉNÉRALES

Article 27

L'article 27 du PL64 introduit un nouveau droit, soit la portabilité des données. Ce droit confère à la personne concernée le droit de recevoir dans un format technologique structuré et couramment utilisé, les renseignements personnels qui la concernent. Contrairement au droit à la portabilité de l'article 20 du RGPD, le PL64 ne limite pas ce droit uniquement aux renseignements collectés par des procédés automatisés. Seul l'alinéa 3 de l'article 27 atténue ce droit en précisant qu'une entreprise peut s'y soustraire s'il y a des difficultés pratiques sérieuses. Ce critère n'est pas objectif et il est difficile pour une entreprise de s'assurer qu'il est respecté au moment où le droit est exercé. Considérant les importantes sanctions que peut subir une entreprise qui ne respecte pas ce droit, il serait important que les critères d'application soient clarifiés.

Il est important que le droit à la portabilité se limite aux renseignements personnels de la personne concernée. Il faut éviter que ce droit devienne une façon d'obtenir des informations commerciales sensibles, d'autant plus que les systèmes technologiques demeurent un outil de concurrence important pour les entreprises. Cette précision apparaît à la page 4 de l'*Analyse d'impact réglementaire*[17], qui indique : « Ce droit ne vise pas les renseignements qui sont 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. ». Aucune mention n'est faite à cet égard dans le PL64. **Le BAC recommande de préciser que les informations commerciales générées, tel qu'indiqué dans l'Analyse d'impact, ne sont pas comprises dans le droit à la portabilité.**

Tel qu'il est rédigé, le droit à la portabilité des données du PL64 imposerait une certaine uniformisation des systèmes des technologies de l'information et une coordination dans

[17] Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques, *Analyse d'impact réglementaire*, 30 juillet 2020, p.4.

l'utilisation des systèmes. **Le BAC recommande donc d'inclure un critère objectif en limitant le droit uniquement aux renseignements personnels collectés à l'aide de procédés automatisés, lorsque c'est possible techniquement avec les systèmes existants de l'entreprise**.

Article 32

L'article 32 prévoit que le responsable de la protection des renseignements personnels doit répondre à la demande d'accès ou de rectification. Le BAC est d'avis que la Loi ne devrait pas indiquer qui doit répondre à la demande. Les entreprises devraient avoir la latitude de déterminer qui, selon leur cadre de gouvernance, est la meilleure personne pour répondre à cette demande. **Le BAC recommande donc de modifier l'article 32 comme suit :**

> **« L'entreprise doit répondre par écrit à la demande d'accès ou de rectification, avec diligence et au plus tard dans les 30 jours de la date de réception de la demande. »**

Article 40.1

Le critère prévu à l'article 40.1, soit « si la connaissance de ce renseignement est susceptible d'aider le requérant dans son processus de deuil » est un critère subjectif. Considérant qu'une entreprise qui communique des renseignements à un tiers en contravention à la Loi peut faire l'objet d'une amende en vertu de l'article 91 paragraphe 1, le BAC propose que le critère de l'article 40.1 soit laissé à la discrétion de la Commission d'accès à l'information (CAI).

À cet égard, le BAC recommande de modifier l'article 40.1 comme suit :

> **« Une personne qui exploite une entreprise peut communiquer au conjoint ou à un proche parent d'une personne décédée un renseignement personnel qu'elle détient concernant cette personne si la connaissance de ce renseignement est susceptible d'aider le requérant dans son processus de deuil et que la Commission d'accès à l'information le lui demande par écrit. »**

SECTION V
RECOURS

§ 2. — DÉCISION DE LA COMMISSION

Article 58

Le BAC recommande de modifier l'alinéa 2 de l'article 58 afin que la décision qui ordonne à une partie de s'abstenir de faire quelque chose devienne exécutoire uniquement à la date de réception de cette ordonnance. Ainsi, l'événement qui déclencherait l'ordonnance serait identique à l'alinéa 1 de l'article 58.

SECTION VII
APPLICATION DE LA LOI

§ 4.1. — SANCTIONS ADMINISTRATIVES PÉCUNIAIRES

Article 90.12

L'article 90.12 du PL64 introduit des sanctions administratives pécuniaires démesurées qui ne reflètent pas le marché et la réalité québécoise. Les montants prévus au PL64 sont identiques à ceux prévus à l'article 83 paragraphe 4 du RGPD alors que le marché européen est très différent du nôtre.

Plusieurs lois québécoises comportent des sanctions, mais celles-ci ne se comparent d'aucune façon à ce que prévoit le PL64. Par exemple, les sanctions administratives pécuniaires prévues à la *Loi sur la qualité de l'environnement*[18] et dans la *Loi sur les assureurs*[19] ne dépassent pas 10 000 dollars. L'objectif de ce type de sanction est de favoriser une culture de conformité à la loi au sein de l'entreprise.

De plus, l'indicateur basé sur un « chiffre d'affaires mondial » n'est pas clair. Si ce critère est retenu, une définition devrait être introduite afin d'éviter différentes interprétations.

Le BAC recommande de modifier l'article 90.12 afin de limiter les montants des sanctions administratives pécuniaires à des montants semblables à ceux qui se retrouvent dans la *Loi sur les assureurs* et la *Loi sur la qualité de l'environnement*.

Article 91

Le PL64 modifie les montants des amendes pour les harmoniser avec ceux prévus au RGPD. Le BAC réitère que le marché québécois est très différent du marché européen. **À cet égard, le BAC recommande de réduire le montant des amendes pour refléter le marché québécois.** Par exemple, la *Loi sur les assureurs* prévoit des peines pour les entreprises ne dépassant pas 2 millions de dollars pour une première infraction[20].

Le BAC recommande donc de réduire le montant des pénalités afin qu'il s'harmonise avec les peines prévues dans les autres lois québécoises.

§ 6. — DOMMAGES-INTÉRÊTS

Article 93.1

Le PL64 introduit un droit privé d'action basé sur la violation statutaire de la *Loi sur le secteur privé* alors qu'il prévoit déjà des mécanismes importants de sanctions contre les entreprises qui ne se conforment pas à celle-ci. D'autre part, les principes de responsabilité civile établis par l'article 1457 du *Code civil du Québec* s'appliquent dans tous les cas où un préjudice est causé, et conséquemment, le BAC se questionne sur la nécessité d'introduire le premier alinéa de l'article 93.1 et demande le retrait de celui-ci.

Quant à l'alinéa 2 de l'article 93.1, le BAC est d'avis que les dommages-intérêts punitifs devraient se limiter à des atteintes intentionnelles, comme prévu à l'article 49 de la *Charte des droits et libertés de la personne*[21], et non à des fautes lourdes.

Le BAC est également d'avis que le PL64 ne devrait pas prévoir de montant minimum pour les dommages-intérêts punitifs. En effet, l'article 1621 du *Code civil* prévoit que le montant des dommages-intérêts punitifs ne devrait pas excéder la valeur de ce qui est suffisant pour assurer

[18] RLRQ c Q-2.
[19] Article 494 de la *Loi sur les assureurs*.
[20] Article 516 de la *Loi sur les assureurs*.
[21] RLRQ c C-12.

leur fonction préventive. À cet égard, le BAC est d'avis que cette détermination devrait être laissée entièrement à la discrétion du tribunal.

Le BAC recommande de :

- **Retirer l'alinéa 1 de l'article 93.1;**
- **Modifier l'alinéa 2 de l'article 93.1 afin de retirer un montant minimum pour les dommages-intérêts punitifs;**
- **Modifier l'alinéa 2 de l'article 93.1 afin de retirer « résulte d'une faute lourde ».**

Article 165

Le BAC recommande de modifier les dispositions transitoires pour prévoir de nombreux droits acquis tels qu'ils sont identifiés à plusieurs endroits dans le mémoire.

CONCLUSION

Le BAC réitère l'importance de moderniser les lois en matière de protection des renseignements personnels. Par ailleurs, cette modernisation doit se faire de façon harmonisée avec les dispositions applicables dans le reste du Canada, notamment en ce qui concerne la divulgation des incidents de confidentialité et le transfert des renseignements personnels dans une autre juridiction. À cet égard, le BAC est persuadé que le succès du RGPD réside dans l'harmonisation des règles de droit des 27 pays membres, en permettant la libre circulation des renseignements personnels entre ces pays et une concurrence équitable entre les entreprises de ce vaste marché.

Le gouvernement doit également s'assurer de la cohérence entre les encadrements législatifs applicables aux entreprises et éviter tout fardeau de conformité excessif. Les assureurs de dommages sont déjà soumis à de nombreuses dispositions spécifiques à leurs activités et certaines sont en contradiction avec le PL64 tel que démontré précédemment.

Le BAC insiste sur la disproportion des sanctions proposées dans le PL64. Celles-ci doivent impérativement être adaptées au marché et à la réalité économique du Québec.

Le BAC est persuadé que les consultations qui auront lieu dans les prochains mois permettront d'apporter au PL64 les modifications nécessaires afin que l'ensemble des dispositions applicables soit cohérent, équitable et harmonisé.

Finalement, nous vous remercions de l'opportunité que vous donnez aux assureurs de dommages de commenter ce projet de loi, par l'intermédiaire du BAC.