IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

1250 René-Lévesque Ouest | Bureau 2200
Montréal (Québec) | H3B 4W8

Tél. 514.843.8950

www.accvm.ca

Susan Copland, LL. B., B. Comm.
Directrice générale
scopland@iiac.ca

Annie Sinigagliese, CPA, CA, FCSI
Directrice générale, Relations Gouvernementales
asinigagliese@iiac.ca

Le 23 septembre 2020

PAR COURRIEL

L'Honorable Simon Jolin-Barrette
Ministre de la Justice
ministre@justice.gouv.qc.ca

Commission des institutions
Assemblée Nationale du Québec
ci@assnat.qc.ca

Objet : Projet de loi n° 64 du Québec, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (le projet de loi ou les propositions)

Monsieur le Ministre,

L'Association canadienne du commerce des valeurs mobilières (l'ACCVM) est reconnaissante d'avoir la possibilité de commenter le projet de loi. L'ACCVM est l'association nationale qui représente 114 sociétés de courtage en valeurs mobilières en matière de règles et de politiques sur les valeurs mobilières. Les membres de l'ACCVM sont des intermédiaires indispensables sur les marchés financiers canadiens. Ils sont responsables de la grande majorité : des services-conseils en finance fournis aux investisseurs; des activités de négociation et de prise ferme de valeurs mobilières sur les marchés boursiers et privés pour le compte des gouvernements et des entreprises.

Les membres de l'ACCVM fournissent des services-conseils en finance à des millions de Canadiens. Ils détiennent 6 615 000 comptes de courtage de plein exercice, en plus de plusieurs comptes autogérés, comptes en ligne et comptes hybrides. Notre secteur protège les renseignements personnels – dont certains sont parmi les plus sensibles – des titulaires de comptes, notamment le détail des comptes, l'accès aux comptes, les données financières.

La révolution numérique en cours a engendré, et continuera d'engendrer, d'importantes répercussions sur le quotidien des gens et sur les activités de presque toutes les entreprises. Les règles sur l'utilisation des données ont une influence considérable sur les activités commerciales. La réglementation a un impact sur les décisions d'affaires fondamentales, notamment sur la faisabilité commerciale de fournir des services utiles personnalisés aux clients en fonction du cadre réglementaire qui pourrait être mis en place pour protéger leurs données. C'est pourquoi il est indispensable qu'au lieu d'imposer les mêmes exigences à tous les secteurs, la réglementation proposée tienne compte des différences entre les secteurs concernant l'utilisation de la technologie et des données pour leur permettre d'élaborer les meilleures pratiques.

Nous sommes profondément préoccupés par un certain nombre d'articles du projet de loi qui sont incompatibles avec les réglementations sur la protection de la vie privée en vigueur au pays et à l'étranger, qui sont extrêmement contraignants au point d'être pratiquement impossibles à opérationnaliser, et qui ne protègent pas adéquatement les données des investisseurs.

Un principe de base de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est la nécessité de trouver un juste équilibre entre la protection de la vie privée et l'utilisation commerciale des données. L'objectif est d'encourager le développement d'une économie numérique et de solutions technologiques qui sont indispensables à la mise en place d'une économie forte et compétitive. Contrairement à la LPRPDE et au *Règlement général sur la protection des données* (RGPD) de l'Union européenne, le projet de loi ne mentionne pas le principe du juste équilibre, qui est essentiel selon nous.

Nous demandons instamment au gouvernement du Québec de travailler avec le ministère de l'Innovation, des Sciences et du Développement économique du Canada (ISDE) et les organismes provinciaux pertinents de la Colombie-Britannique, de l'Alberta et de l'Ontario afin de mettre au point une réglementation sur la protection de la vie privée harmonisée à la grandeur du Canada. Actuellement, les lois fédérale et provinciales en matière de protection de la vie privée sont relativement semblables sur le plan du contenu et des résultats. Introduire des incompatibilités accroît l'incertitude, entraîne des inefficiences, augmente les coûts de conformité des entités canadiennes qui exercent des activités commerciales au Canada, augmente les coûts de conformité des entités étrangères qui veulent faire des affaires au Canada, et ce, sans valeur ajoutée pour l'investisseur. L'harmonisation facilite aussi les interactions avec le RGPD et d'autres réglementations internationales qui reconnaissent les juridictions dont les règles sont conformes au RGPD et à ces autres réglementations internationales.

Certains éléments du projet de loi préoccupent grandement notre secteur, le secteur des valeurs mobilières.

Responsabilisation

La *Loi sur la protection des renseignements personnels dans le secteur privé* actuellement en vigueur au Québec diffère de la LPRPDE, car elle ne responsabilise pas les entreprises dans les efforts de conformité qu'elles déploient pour s'y conformer. Certes, un certain nombre d'articles du projet de loi prévoient que les entreprises doivent adopter des mesures de gouvernance précises en matière de protection de la vie privée. Cependant, le projet de loi ne laisse pas suffisamment de souplesse aux entreprises pour qu'elles puissent établir elles-mêmes les mesures de sécurité sur le plan des politiques et des procédures qui conviennent à leurs activités. De telles mesures responsabiliseraient les entreprises en les tenant responsables de la réalisation des objectifs de ces mesures.

Comme indiqué ci-dessus, un moyen de responsabiliser les entreprises est de faciliter – sous la supervision du régulateur du secteur le cas échéant – la création de meilleures pratiques adaptées à chaque secteur en tenant compte des particularités de chaque secteur en matière de collecte et d'utilisation de données.

Politiques et pratiques

Pour favoriser la transparence et une certaine responsabilisation, le projet de loi prévoit qu'au Québec les entreprises établissent, mettent en œuvre et publient des politiques et des pratiques de gouvernance sur la protection des renseignements personnels. Ces politiques doivent être exhaustives et très détaillées en ce qui concerne les opérations et les processus internes. Certes, il est approprié que les entreprises élaborent des politiques internes détaillées en matière de traitement de données. Cependant, il est inapproprié d'exiger que les entreprises publient leurs politiques et processus en matière de traitement de données. De plus, il est de pratique courante que les organisations publient sur leur site internet des politiques et des avis en matière de protection de la vie privée conformément aux exigences de transparence de la LPRPDE. Cependant, la publication de politiques et de procédures internes détaillées en matière de protection de la vie privée n'est pas de pratique courante. En outre, une telle publication n'est pas utile au public à cause de l'ampleur et de la complexité de telles informations. De plus, les politiques peuvent contenir des renseignements qui font l'objet d'une concurrence entre les entreprises, ce qui constitue une autre raison pour ne pas publier les informations détaillées.

Consentement

Nous sommes extrêmement inquiets face aux exigences plus strictes en matière de consentement prévues dans le projet de loi, particulièrement les exigences qui s'appliquent à la circulation transfrontalière des données et aux multiples fournisseurs de services qui font le traitement des données. Nous étions en désaccord avec le Commissariat à la protection de la vie privée du Canada (le Commissariat) lorsqu'il avait proposé de semblables exigences en 2019. Après avoir reçu beaucoup de commentaires, le Commissariat a retiré sa proposition. Le Commissariat a reconnu les difficultés d'obtenir un consentement distinct avant de pouvoir recueillir, utiliser et communiquer des renseignements personnels. Le 4 août 2020, le Commissariat a publié les Conclusions en vertu de la LPRPDE n° 2020-001 qui confirment que l'obtention d'un consentement distinct n'est pas nécessaire pour le traitement transfrontalier de données.

Étant donné la quantité importante de données qui sont recueillies et utilisées de façon de plus en plus innovatrice grâce à l'évolution technologique rapide, l'obligation d'obtenir un consentement distinct et détaillé chaque fois qu'une donnée est utilisée pour fournir un produit ou un service est inexécutable et inefficiente, et il sera pratiquement impossible de l'opérationnaliser.

Plutôt que d'exiger un consentement distinct, nous sommes d'avis qu'il est plus approprié de se fier à la responsabilité de l'entité pour laquelle les données sont recueillies et utilisées ainsi qu'à la responsabilité des entités (fournisseurs de services) qui traitent les données de l'entité pour laquelle les données sont recueillies et utilisées. Les dispositions législatives fédérales associées à la LPRPDE sont basées sur ces responsabilités. Il n'est pas nécessaire d'exiger un consentement distinct uniquement pour transférer des données à des fins de traitement ni pour autoriser une circulation transfrontalière de données. Il est plus approprié de prévoir une exception à l'obtention du consentement qui correspond aux pratiques commerciales standards pour des services qui font l'objet du contrat que le client a conclu. Il s'agit d'une protection des données des clients qui est conforme à leurs attentes raisonnables.

Les exigences de consentement proposées créent un décalage réglementaire entre le Québec et la réglementation sur la protection de la vie privée des autres provinces et d'organismes internationaux, ainsi qu'un chevauchement du régime canadien de responsabilité et du régime de consentement. Certes, il y a une certaine similarité avec l'obtention obligatoire du consentement prévu au RGPD. Cependant, l'obtention obligatoire du consentement prévue au RGPD s'applique seulement dans des circonstances particulières. En outre, le RGPD accorde des exceptions à l'obtention obligatoire du consentement lorsqu'il s'agit du traitement de données, notamment en matière d'intérêts commerciaux légitimes, ce que ne prévoit pas explicitement le projet de loi. Cette incompatibilité rend le projet de loi beaucoup plus contraignant que la LPRPDE, la *Loi sur la protection de la vie privée et des renseignements personnels de la Colombie-Britannique* (LPVPRP), la LPVPRP de l'Alberta et le RGPD.

Nous sommes particulièrement préoccupés par l'article qui prévoit que le consentement doit être demandé pour chaque utilisation distincte et qu'il doit être demandé séparément de toute autre information communiquée à la personne concernée. Dans un secteur axé sur les données, comme le secteur des valeurs mobilières, les services offerts exigent plusieurs traitements de données effectués par plusieurs fournisseurs de services. En outre, la technologie est en constante évolution et de nouvelles applications pour améliorer les services ne cessent d'apparaître sur le marché. Dans un tel contexte, les clients du secteur des valeurs mobilières seront aux prises avec un nombre écrasant de demandes de consentement, sans cesse renouvelées, générées par les multiples applications qui utilisent des données. Ces applications, dont se servent les nombreux fournisseurs de services qui traitent des données, sont nécessaires pour que les membres de l'ACCVM puissent offrir des services de qualité aux investisseurs. C'est une contrainte insurmontable pour le client qui doit lire, comprendre et approuver de longs descriptifs de politiques, parfois complexes, en matière de protection de la vie privée qui varient inévitablement en fonction de l'entreprise et du secteur.

En outre, des cybercriminels pourraient profiter de la prolifération des demandes de consentement pour installer des logiciels malveillants et commettre un cybercrime. De plus, en Europe, des cybercriminels se sont servis de certains articles du RGPD pour surcharger les gestionnaires de données de demandes de renseignements personnels.

Impact sur le secteur des valeurs mobilières

Le secteur des valeurs mobilières gère une grande quantité de données, notamment : des informations sur les activités bancaires, les actifs, les emprunts, les impôts; des données d'identification personnelle; des informations sur les membres de la famille; d'autres informations nécessaires à la planification financière des clients et pour leur fournir des services de gestion de placement. Effectuer la prestation de services aux investisseurs nécessite l'intervention, dans le processus de placement, de plusieurs tiers pour le traitement des données. Les données sont regroupées, ventilées, analysées, classées, traitées, entreposées avant d'entreprendre, et pour réaliser, les nombreuses étapes que comportent le placement, les activités de négociation, le règlement et la compensation de transactions, la rédaction de rapports, la conformité.

Pour protéger ces données sensibles, les sociétés de courtage en valeurs mobilières ont élaboré des mesures de sécurité et des processus rigoureux en matière de protection des données qu'elles appliquent à l'interne et dans leurs rapports avec les tiers effectuant le traitement des données. De plus, les membres du secteur collaborent étroitement avec le régulateur du secteur, l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), pour bien protéger les données des clients.

Apporter des changements importants à des processus bien établis en matière de gestion de la protection des données des clients nuira aux efforts déployés par les sociétés de courtage dans ce domaine, ce qui pourrait entraver ou même bloquer l'accès des clients aux services financiers offerts par la société avec laquelle ils font affaire.

Au Canada, il y a actuellement 6,6 millions de comptes de courtage de plein exercice. Le consentement est obtenu lorsque le client décide de faire affaire avec la firme de courtage. Ce consentement s'applique à toutes les fins et utilisations probables prévues au moment du consentement. En vertu de la LPRPDE, une utilisation de données qui n'avait pas été prévue lorsque le client a décidé de faire affaire avec une entreprise exige l'obtention d'un nouveau consentement. Cependant, en règle générale, le consentement fourni par le client au moment de faire affaire avec une société de courtage est tellement complet que de nouveaux consentements sont rarement requis. Il est pratiquement impossible pour une société de courtage d'établir et de continuellement mettre en œuvre les activités suivantes concernant les fournisseurs de services qui traitent les données : aviser et obtenir d'autres consentements chaque fois qu'elle fait affaire avec un « nouveau fournisseur traitant des données » – alors que « l'activité de traitement des données » reste la même ; pourvoir aux désistements le cas échéant; exercer le suivi.

Obliger une firme à fournir de nouvelles informations aux clients et à obtenir de nouveaux consentements lorsqu'il s'agit d'un compte existant impliquera de modifier le libellé des documents du compte en ce qui a trait au consentement, ce qui non seulement est irréaliste, mais en plus causera probablement une interruption à la prestation de services ou des retards pour plusieurs clients qui pourraient ne pas être au courant du déluge de demandes de consentements exigées par le projet de loi. Cela risque d'être très préjudiciable aux clients, car tout délai de négociation sur les marchés financiers est susceptible d'être crucial.

Nous sommes d'avis que les propositions ne représentent pas un juste équilibre entre la protection additionnelle offerte à l'investisseur et l'importante contrainte imposée aux sociétés de courtage et à leurs clients.

Les investisseurs s'attendent raisonnablement à ce que les sociétés de courtage en valeurs mobilières aient mis en place des processus de sécurité appropriés et qu'elles se soient organisées pour que les tiers avec lesquels elles font affaire protègent aussi les données de leurs clients. Exiger le consentement exprès du client pour transférer des données aux fins de traitement n'ajoute pas de protection additionnelle. Le consommateur aura toujours le dernier mot : il fait confiance à la société de courtage en valeurs mobilières avec laquelle il fait affaire ou il résilie le contrat avec elle.

Une approche pratique et efficace est de prévoir des exceptions à l'obtention du consentement pour les pratiques commerciales standards nécessaires à la prestation du service demandé par le client. En cas de problème, la société de courtage et les fournisseurs traitant des données doivent être responsables.

Plutôt qu'exiger la mise en œuvre d'un régime de consentement plus rigoureux, nous recommandons de mettre l'accent sur les renseignements fournis par les organisations. Celles-ci devraient utiliser un langage simple pour décrire comment elles utiliseront les données du client dans le cadre de leurs activités commerciales.

Nous sommes d'avis que, pour que les renseignements personnels soient utilisés de façon appropriée et conformément aux attentes du client, il est plus efficace d'exiger que les entreprises fournissent des renseignements raisonnables et de les tenir responsables de leur utilisation des renseignements du client – ce que prévoit la LPRPDE. La responsabilité prévue dans la LPRPDE est un élément indispensable pour que les organisations se conforment aux règles sur la protection de la vie privée. Exiger de l'investisseur qu'il fournisse d'autres consentements ne permettra pas d'atteindre l'objectif fondamental qui est la protection des données des clients et n'offrira pas aux clients d'autres options pour le traitement des données. D'ailleurs, chaque fois qu'un client fournit un consentement exprès, il assume en fait une certaine responsabilité, ce qui contrevient au principe de la responsabilité des entreprises en matière de données qui est au cœur du régime canadien sur la protection de la vie privée et du régime instauré par le RGPD. On pourrait aussi faire valoir qu'il y a un transfert de responsabilité de l'utilisateur de données vers le client « consentant », ce qui atténuerait les dommages subis en cas de litige découlant d'un transfert de données. Tout allègement de la responsabilité des entreprises ou toute diminution de préjudice sont contraires aux intérêts des consommateurs et à l'objectif et à la raison d'être du projet de loi.

Nous sommes cependant d'accord que l'obtention d'un consentement distinct est indispensable à la transparence et responsabilité des entreprises lorsque des données à caractère personnel sont utilisées à des fins qui ne font pas partie de l'entente de prestation de services à laquelle s'est engagé le client, par exemple lorsque les données sont fournies à un tiers qui n'a rien à voir avec les services convenus avec le client.

En ce qui concerne la circulation transfrontalière des données, l'obligation d'obtenir le consentement est inexécutable pour les firmes de courtage. Plusieurs tâches reliées au traitement des données, notamment les applications infonuagiques, sont effectuées dans des juridictions hors Québec. Les règles sur la circulation transfrontalière des données ne devraient pas être différentes des règles sur les autres activités de traitement des données. Elles devraient être assujetties aux règles générales sur les renseignements à fournir aux clients et sur la responsabilité des entreprises. En outre, le fait qu'une opération effectuée au Canada – d'une province à une autre – soit considérée comme « transfrontalière » est particulièrement discutable et inutile, étant donné la robustesse et l'harmonisation du régime réglementaire canadien pour les valeurs mobilières.

Aussi discutable est l'article du projet de loi qui prévoit que lorsque la législation d'une autre juridiction n'est pas du même « degré d'équivalence », le transfert d'informations est interdit et il ne peut pas être effectué même si le client consent au transfert.

Nous nous inquiétons de l'obligation imposée aux entreprises d'établir elles-mêmes le caractère adéquat du régime de protection de la vie privée des autres juridictions. Il s'agit d'une autre obligation inexécutable. Les entreprises n'ont ni la compétence, ni les ressources pour établir le degré d'équivalence du régime de protection de la vie privée des autres juridictions. En outre, il y a un risque important de discordance entre les différentes entités sur leur évaluation du caractère adéquat desdits régimes.

Absence d'exception à l'obtention du consentement des employés

Nous constatons que le projet de loi ne prévoit pas une exception à l'obtention du consentement des employés. La LPRPDE, la LPVPRP de la Colombie-Britannique, la LPVPRP de l'Alberta autorisent les employeurs à recueillir, utiliser, communiquer – sans le consentement des employés – les renseignements personnels des employés nécessaires à l'embauche, en cours d'emploi, à la cessation d'emploi. Les employeurs ont cependant l'obligation d'informer les employés de leurs pratiques. Une exception devrait être disponible.

Renseignement personnel sensible

Nous sommes d'avis que le terme « renseignement personnel sensible » ne devrait pas être défini, car il est probablement tributaire du contexte et de d'autres renseignements recueillis en même temps ou plus tard. Définir le terme « renseignement personnel sensible » et ajouter d'autres « protections » augmentera les contraintes sans ajouter de nouvelles protections véritables, particulièrement s'il s'agit de renseignements nécessaires à la prestation de services convenus et que leur utilisation est conforme aux attentes raisonnables du client. On doit se fier, là encore, à la responsabilité des entreprises pour garantir la sécurité des données.

Obligation de procéder à l'évaluation des facteurs relatifs à la vie privée

Nous sommes en désaccord avec l'obligation des entreprises de réaliser une « évaluation des facteurs relatifs à la vie privée » à l'égard de tout « projet de système d'information » ou de tout « projet de prestation électronique de services » concernant le traitement d'un renseignement personnel (article 3.3). L'obligation est beaucoup trop générale et elle n'est pas assujettie à un seuil

d'importance relative, à la différence de l'article 35(1) du RGPD qui prévoit qu'une analyse de l'impact des opérations de traitement envisagées doit être effectuée seulement si le traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Protection de la vie privée dès la conception

Nous sommes d'accord qu'il est approprié d'assujettir à l'exigence de protection de la vie privée dès la conception les entreprises qui recueillent des renseignements personnels en offrant un produit ou un service technologique. Cependant, la règle édictée dans les propositions – « Une personne qui exploite une entreprise et qui recueille des renseignements personnels en offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou de ce service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée » – est discutable. La règle ne tient pas compte du profil de risque : du système, des renseignements, de la technologie. Le coût des mesures de protection des données nécessaires pour se conformer à la règle proposée est susceptible d'être excessif si on l'applique à tous les systèmes sans tenir compte de la fonction de chacun.

En outre, la règle est incompatible avec le RGPD qui prévoit explicitement que l'on doit tenir compte des circonstances de chaque cas, notamment « les coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger ».

Nous sommes aussi préoccupés par la norme du « plus haut niveau de confidentialité ». Il s'agit d'une norme nouvelle qui n'a pas actuellement d'équivalence dans les règles sur la protection de la vie privée en vigueur de par le monde. L'article 9.1 proposé ne fournit aucune indication sur le contenu du « plus haut niveau de confidentialité » en fonction du contexte. Nous recommandons d'ajouter dans l'article un critère de raisonnabilité qui tient compte des considérations commerciales raisonnables et du modèle d'affaires.

Obligation de signaler un incident de confidentialité

Nous sommes d'accord avec les nouvelles exigences de signalement obligatoire d'un incident de confidentialité prévues dans les propositions. Cependant, il est indispensable que les exigences soient harmonisées avec les exigences de la LPRPDE et des autres règlements pertinents en matière de protection de la vie privée pour éviter que les entreprises ne soient assujetties, pour le même incident de confidentialité, à des exigences, des éléments déclencheurs, des seuils différents, alors qu'elles sont occupées à minimiser et à mettre fin aux dommages causés par l'incident de confidentialité. Nous recommandons de modifier le libellé du seuil de « l'incident de confidentialité » en remplaçant « risque qu'un préjudice sérieux soit causé » par le libellé de la LPRPDE : « risque réel de préjudice grave ».

Obligation d'informer les individus de l'utilisation des technologies permettant l'identification, la localisation ou le profilage

Le secteur des valeurs mobilières se distingue par l'utilisation d'outils d'analyse de données pour offrir aux individus des produits et des services financiers personnalisés avantageux en fonction de leur profil. La capacité du secteur de mener pour les clients ces importantes activités de personnalisation sera sérieusement compromise par le projet de loi.

Certes, il est raisonnable qu'une entreprise informe de manière générale ses clients qu'elle utilise une technologie qui permet l'identification, la localisation et le profilage des individus. Cependant, il est tout à fait irréaliste d'exiger qu'une entreprise identifie chaque activité de traitement susceptible de créer ou d'utiliser le profilage. De plus, il est impossible qu'une entreprise puisse fournir un service si les fonctions qui lui permettent de le fournir ont été désactivées pour se conformer au présent projet de loi.

Portabilité des données

L'ACCVM a des questions et des réserves sur le droit explicite que le projet de loi accorde aux individus d'obtenir que leurs renseignements personnels soient transmis d'une organisation à une autre dans un format numérique normalisé. Nous sommes d'accord avec la mobilité des données lorsqu'il s'agit d'aider les individus à contrôler leurs données et de fournir aux entreprises un moyen efficient pour gérer les renseignements sur les consommateurs. Cependant, les données assujetties à ces articles doivent être clairement et étroitement définies pour : opérationnaliser la gestion de ces données; éliminer le risque d'erreur; éliminer le risque de communication inappropriée. Par exemple, le processus de transfert d'une organisation à l'autre d'un sous-ensemble précis de renseignements devrait être sans ambiguïté. Ce ne sont pas tous les renseignements sur le consommateur dont a besoin l'organisation destinataire ou dont la détention par l'organisation destinataire est appropriée.

Un effet involontaire possible de la mobilité des données ne se limitant pas à des informations spécifiques pourrait être de multiplier le nombre de bases de données contenant des informations sur des individus, plutôt que d'en limiter le nombre. Cela pourrait se produire si les entreprises séparent les types de données qu'elles détiennent sur les individus. Par exemple, les entreprises pourraient séparer les données de base fournies par le client des données provenant de systèmes d'analyse. Ceci serait fait pour s'assurer qu'elles limitent certains types d'informations qui pourraient être soumises à des demandes de mobilité de données.

Nous recommandons de définir clairement les sous-ensembles de données à transférer pour que seules les données appropriées et pertinentes soient transférées entre les organisations. Nous sommes d'accord avec la proposition de restreindre les données transférées aux seuls renseignements fournis par l'individu. L'information dérivée ou les renseignements fournis par un tiers doivent être exclus.

Les articles sur la mobilité des données devraient différencier les organisations selon la présence de normes techniques appropriées (compatibilité, authentification, sécurité des données) et de contrôles pertinents. L'échéancier de mise en œuvre des règles sur la mobilité des données doit tenir compte du temps nécessaire pour mettre au point les normes du secteur.

D'un point de vue pratique, les données qui seront assujetties aux règles sur la mobilité des données devront être regroupées en fonction des secteurs. Par exemple, les données personnelles confiées à une société financière ne devraient être partagées qu'avec d'autres sociétés financières. Ces renseignements personnels ne devraient pas, par exemple, être partagés avec des prestataires de soins de santé. En établissant des sous-ensembles de données, ce qui restreint du même coup la mobilité des données, on minimise le risque d'un détournement de données. De plus, il sera plus facile de standardiser en fonction des secteurs les bons sous-ensembles, normes et formats de données parce que les organisations du même secteur utilisent déjà des programmes et protocoles semblables pour communiquer entre elles et partager de l'information. Il est irréaliste d'imposer des normes technologiques, des protocoles et des

formats semblables pour tous les secteurs dans lesquels des données personnelles sont recueillies, entreposées, utilisées, de façon et à des fins très différentes.

Droit à l'oubli

Certes, nous sommes d'accord pour que les individus détiennent un certain degré de contrôle sur leurs données une fois que l'objectif relié à la communication des données est atteint. Cependant, nous sommes préoccupés par les contraintes opérationnelles importantes que les propositions imposent aux secteurs dont les entreprises : utilisent les données pour toute une gamme de fonctions dans les différents services de l'entreprise; font affaire avec des fournisseurs de services traitant des données pour la prestation de services.

Par exemple, les sociétés du secteur des valeurs mobilières recueillent une quantité importante de données au sujet de leurs clients dans le but de leur offrir des placements à haute valeur ajoutée, des services de planification financière et des services de négociation appropriés à la situation du client. Les informations recueillies ne sont pas rendues publiques. Elles sont utilisées uniquement au sein de la société de courtage et communiquées uniquement aux tiers traitant des données. Ces fournisseurs de services qui font le traitement des données sont nécessaires à la prestation des services convenus avec le client.

Il faut par ailleurs noter que les organismes d'autoréglementation qui régissent les professionnels en placement et les membres de l'ACCVM ont élaboré des règles en matière de rétention et de suppression pour superviser étroitement le fonctionnement du secteur et pour tenir compte des attentes des clients. Certaines règles prévues dans le projet de loi sont incompatibles avec des règles présentement en vigueur dans le secteur des valeurs mobilières. Il y aura donc de graves problèmes de conformité concernant les données : qui sont utilisées de différentes façons dans la même société de courtage; qui sont communiquées aux fournisseurs qui traitent des données pour la prestation de divers services au client, par exemple les activités de négociation, la planification financière, l'épargne-retraite.

Nous croyons que le projet de loi devrait cibler les organisations et les plateformes qui fournissent des renseignements personnels par l'intermédiaire d'un accès public en ligne plutôt que les entreprises qui n'ont pas d'impact sur la réputation en ligne des individus.

Droit de s'opposer au traitement automatisé

Le droit de s'opposer au traitement automatisé prévu à l'article 12.1 du projet de loi ne cadre pas avec l'usage de la technologie pour fournir des services financiers ciblés à haute valeur ajoutée. Les firmes de courtage ne pourraient pas offrir de services si l'analyse automatisée des données n'existait pas dans le secteur. Il est de pratique courante pour les courtiers en valeurs mobilières de se servir du traitement automatisé des renseignements personnels pour optimiser le choix du produit ou du service proposé au client en fonction de sa situation financière, de sa tolérance au risque et de d'autres informations personnelles.

Il est normal de fournir aux individus des informations générales sur le traitement automatisé des données. Cependant, la prépondérance et la complexité des outils d'analyse de données dans le secteur

des valeurs mobilières font qu'il est impossible de fournir aux individus des informations précises et détaillées sur tous les facteurs et paramètres qui interviennent dans une décision automatisée.

Lorsqu'une décision est fondée exclusivement sur un traitement automatisé et que le client croit qu'il y a eu erreur dans le traitement de ses données personnelles, il est approprié de donner « à la personne concernée l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision ».

Sanctions administratives pécuniaires

Nous sommes préoccupés par l'imposition de sanctions administratives pécuniaires (SAP) et par le montant des SAP. Il sera pratiquement impossible de gérer et d'appliquer le système de SAP d'une manière juste et uniforme à cause : de la complexité du projet de loi; des multiples infractions possibles prévues au projet de loi pouvant conduire à l'imposition de SAP; des différentes utilisations de l'information en fonction des secteurs; des disparités dans l'utilisation de l'information à l'intérieur d'un même secteur; du large éventail d'infractions. Le montant élevé des SAP paralysera l'utilisation et le développement des technologies susceptibles d'améliorer les services aux consommateurs. Les SAP sont différentes – et leurs montants sont beaucoup plus élevés – que ce qui est prévu à la LPRPDE et à la réglementation sur la protection de la vie privée en vigueur dans les autres provinces canadiennes.

Dispositions pénales

Nous sommes préoccupés par les montants exorbitants des amendes prévus dans le projet de loi et avec le fait qu'elles s'appliquent à un plus grand nombre d'infractions que celui des SAP. Comme indiqué ci-dessus, nous craignons une paralysie du développement de technologies susceptibles de profiter aux divers secteurs, aux clients, à l'économie en général. Les amendes sont différentes – et leurs montants sont beaucoup plus élevés – que ce qui est prévu à la LPRPDE et à la réglementation sur la protection de la vie privée en vigueur dans les autres provinces canadiennes.

Poursuites en dommages

Nous sommes d'avis que le droit accordé aux individus par le projet de loi de poursuivre une entreprise en dommages est inutile. En cas d'atteinte à la vie privée, il est présentement possible d'intenter des actions en justice devant les tribunaux du Québec en se fondant sur les dispositions du Code civil du Québec relatives à la protection de la vie privée. Accorder un autre droit d'action est susceptible d'augmenter le nombre de recours collectifs en absence de préjudice réel.

Autoréglementation et normes techniques

L'ACCVM note que, contrairement au RGPD et aux propositions de l'ISDE sur la LPRPDE, le projet de loi ne prévoit pas l'utilisation de codes, normes, certifications propres à chaque secteur. Le développement et l'utilisation de codes sectoriels seraient extrêmement utiles pour améliorer la souplesse de la réglementation et afin de favoriser l'innovation responsable. Les codes sectoriels représentent l'uniformité et la prévisibilité lorsqu'il s'agit de faire affaire avec des juridictions qui se fient à ces codes pour superviser les activités commerciales avec les autres juridictions – notamment les juridictions assujetties au RGPD – sans besoin d'imposer d'autres exigences.

Les organisations diffèrent les unes des autres sur le plan de la quantité, de la gestion et de l'utilisation de données. Pour en tenir compte, il est indispensable d'élaborer des codes, normes, certifications qui ne soient pas identiques pour toutes les organisations, car ils doivent être suffisamment souples pour s'adapter aux données entreposées de chaque organisation et à leur utilisation par l'organisation. Pour que les codes, normes, certifications soient pertinents et utilisés dans les divers secteurs, il est important que chaque secteur participe au développement des protocoles et des normes qui y seront applicables.

Les codes et les certifications ne devraient pas être obligatoires mais facultatifs, car il est possible que des organisations ne puissent pas les appliquer ou qu'il ne soit pas avantageux pour des organisations de les adopter. L'utilisation des codes par une entreprise constituera une preuve de l'adoption par l'entreprise de normes appropriées et aidera à juger de sa responsabilité en cas d'atteinte aux renseignements des clients. Toutes les entreprises, particulièrement celles qui gèrent beaucoup de renseignements personnels, seront donc motivées à se conformer aux codes de leur propre secteur.

Nous sommes d'avis que les codes et les certifications devraient être : gérés par un organisme de certification indépendant accrédité par le Conseil canadien des normes; supervisés, le cas échéant, par le régulateur attitré du secteur (comme l'OCRCVM). Les codes seront alors bien appliqués, car le régulateur attitré de chaque secteur sait comment les données sont utilisées et protégées dans son secteur.

Nous recommandons aussi d'ajouter dans le projet de loi des articles sur l'utilisation des codes et des certifications. En cas d'infraction, leur mise en application ou non pourra aider à évaluer les recours appropriés.

Merci de tenir compte de nos commentaires et n'hésitez pas à communiquer avec Annie Sinigagliese au asinigagliese@iiac.ca ou au 514-843-8950 si vous avez des questions.

Veuillez agréer nos salutations distinguées.

Susan Copland

Annie Sinigagliese