Le 3 novembre 2021

Me Diane Poitras
Présidente
Commission d'accès à l'information du Québec
2045, rue Stanley, Bureau 900
Montréal (Québec), H3A 2V4

Objet : Demande de clarifications concernant le projet de loi 64

Madame la Présidente,

Je vous écris au nom de l'Electronic Transactions Association ("ETA") pour obtenir plus d'informations et de précisions sur le projet de loi 64 (*Loi visant à moderniser les dispositions législatives en matière de protection des renseignements personnels*), et sur la façon dont diverses nouvelles obligations pourraient s'appliquer à nos membres.

L'ETA est la principale association professionnelle du secteur des paiements, représentant plus de 500 entreprises qui offrent des produits et services de traitement des transactions électroniques. Les membres de l'ETA incluent des institutions financières, des fournisseurs de services de paiement mobile, des fournisseurs de portefeuilles mobiles et des prêteurs en ligne non bancaires qui accordent des prêts commerciaux, principalement aux petites entreprises, soit directement, soit en partenariat avec d'autres prêteurs. Les entreprises membres de l'ETA créent des solutions innovantes dans le domaine des services financiers, révolutionnant la manière dont le commerce est réalisé grâce à des solutions de paiement et des alternatives de prêt sûres, pratiques et avantageuses.

L'Association a suivi le processus d'adoption du projet de loi 64 afin de mieux comprendre les changements apportés par le gouvernement du Québec et les impacts de ces changements sur les opérations de nos membres au Québec, au Canada et à l'étranger. Nous tenons à remercier le gouvernement du Québec et les députés pour leur approche et leur volonté de répondre aux préoccupations soulevées par l'ETA et ses membres. Cette approche a conduit à l'adoption de modifications pertinentes, notamment la possibilité pour les organisations d'utiliser certains renseignements dans le cadre de leurs activités et au profit des consommateurs (article 102) pour lutter contre la fraude.

Toutefois, certaines des dispositions telles qu'adoptées laissent encore d'importantes questions en suspens, et nous aimerions obtenir des éclaircissements afin de mieux comprendre l'impact du projet de loi sur nos membres et les services qu'ils fournissent littéralement à chaque seconde aux Québécois et aux consommateurs du monde entier.

Nous comprenons que votre organisation pourrait travailler à élaborer des lignes directrices afin de faciliter l'interprétation et la compréhension des nouvelles mesures par les organisations du secteur privé. Dans ce contexte, voici une série de questions et de recommandations qui visent à fournir une rétroaction de l'industrie dans le cadre de cet exercice et pour le développement potentiel de réglementation future :

a) Transfert transfrontalier de données et protection adéquate (article 103).

Cet article prévoit que les renseignements peuvent être communiqués « si l'évaluation démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus ». La notion d'équivalence a été remplacée par la notion d'une protection adéquate. Nos membres aimeraient savoir ce que cette notion signifie concrètement, en quoi est-ce différent de la notion d'équivalence, et comment cette notion s'inscrit quant à la possibilité d'une protection contractuelle ajoutée à l'article 70.1(3).

Dans les cas où une telle évaluation serait requise, ce qui serait considéré comme adéquat n'est pas clair, tout comme la fréquence à laquelle les évaluations de la protection adéquate devraient être menées. Devraient-elles être effectuées pour chaque nouveau renseignement personnel communiqué à l'extérieur du Québec ? Et quelles seraient les obligations lorsque la loi de la juridiction étrangère est modifiée ? Une nouvelle évaluation du caractère adéquat doit-elle être effectuée pour les modifications importantes ? Si oui, dans quel délai ?

Recommandations (article 103)

⇒ *Afin de limiter le fardeau des organisations, notamment des PME, nous croyons que le Québec devrait établir des mécanismes de transfert alternatifs qui ne nécessitent pas d'évaluation, tel que des clauses contractuelles types et des règles corporatives contraignantes.*

⇒ *Nous croyons que l'obligation de procéder à une évaluation devrait être limitée aux transferts transfrontaliers de données à « haut risque », comme ceux qui impliquent un grand volume d'informations sensibles.*

⇒ *Nous croyons que les entreprises devraient être en mesure de définir les « principes de protection des données généralement reconnus » en se fondant sur une liste non exhaustive et flexible de considérations, qui pourrait inclure le degré de similitude entre le système juridique étranger et celui du Québec, la primauté du droit dans le pays étranger, la possibilité de recours efficaces et contraignants et l'adhésion du pays étranger aux cadres juridiques internationaux en matière de protection de la vie privée.*

⇒ *De plus, et conformément à l'accord États-Unis - Mexique - Canada (ACEUM), nous croyons que tous les transferts de données vers les juridictions américaines devraient être considérés comme adéquats de facto. Le gouvernement du Québec devrait préciser qu'il en va de même pour les transferts vers et au sein de toutes les autres provinces canadiennes.*

⇒ *D'après les discussions qui ont eu lieu au cours de votre processus de consultation, nous avons compris qu'une « évaluation du caractère adéquat » distinct n'était pas nécessaire pour chaque renseignement personnel transféré. Il serait très utile que cela soit clarifié/confirmé dans les directives et les règlements.*

b) Le consentement doit être clair, libre, éclairé et donné à des fins précises (article 102)

Le projet de loi prévoit que le consentement doit être demandé pour chaque finalité d'utilisation des renseignements personnels, dans un langage clair et simple et séparément de toute autre information fournie à la personne concernée. Certains de nos membres offrent des services ou travaillent avec des fournisseurs de services qui ne sont pas directement impliqués avec le client, mais qui sont essentiels, pour la protection de la vie privée et la sécurité notamment. Quels seraient la nature et le niveau du consentement requis dans de tels cas? Nous pensons que toute nouvelle mesure ne doit pas devenir un obstacle à l'offre de ces services indirects qui sont essentiels dans l'écosystème. De plus, il n'est pas pratique ni souhaitable que les clients reçoivent des messages demandant un consentement distinct pour chaque type de renseignements personnels recueillis. Cette approche serait unique au Québec et soulèverait plusieurs problèmes pour les entreprises, notamment un développement technique considérable.

Nous comprenons que la deuxième phrase de l'article 14 suggère que le consentement ne peut être demandé dans le cadre d'une politique de confidentialité. À cet égard, comment une politique de confidentialité claire et simple est-elle considérée par cette section ? En outre, comment le consentement implicite est-il pris en compte par l'article 14 ?

L'article 102 prévoit une dérogation spécifique au consentement explicite nécessaire à la prévention ou à la détection de la fraude. D'autres juridictions, y compris le RGPD et la loi sur la protection de la vie privée de l'État américain de Californie, permettent à une entité de refuser une requête de renseignements personnels sur la base d'une exemption pour fraude. Par exemple, si une entité (comme un réseau de paiement) doit conserver les données d'une personne pour lutter contre la fraude, en vertu des lois précédemment citées, elle n'a pas à répondre à une demande de suppression des données qui relève de l'exemption. Cette exemption particulière permet à l'entité de disposer de capacités de prévention de la fraude plus efficaces et contribue à réduire les enjeux liés à la fraude, incluant au niveau des pertes de revenus et des dépenses opérationnelles.

Recommandation (article 102)

⇒ *Nous croyons que si les politiques de confidentialité sont claires et simples, elles sont des véhicules optimaux pour garantir que les clients comprennent comment l'entreprise se propose de collecter, d'utiliser et de divulguer leurs informations.*

⇒ *Les directives devraient étendre l'exemption relative à la prévention de la fraude pour permettre à une entité de refuser la demande d'accès ou de correction des données d'une personne lorsque cela est nécessaire pour maintenir un niveau élevé de prévention de la fraude.*

c) Sanctions pénales et administratives (article 150).

Le cumul des sanctions entre juridictions en cas d'incident de sécurité n'a pas été abordé en détails par la Commission des institutions de l'Assemblée nationale du Québec lors de son étude détaillée. Une entreprise pourrait-elle être sanctionnée plus d'une fois pour le même incident dans plusieurs juridictions différentes ?

Recommandation (article 150)

⇒ *Nous croyons que des mécanismes clairs doivent être mis en œuvre pour éviter que des sanctions soient imposées pour la même infraction dans différentes juridictions, ce qui pourrait donner lieu à des conséquences disproportionnées et à des sanctions inapplicables.*

d) Le plus haut niveau de confidentialité (article 100).

Cet article exige une approche de « désactivation par défaut » pour presque tout produit ou service impliquant le traitement de données, indépendamment du contexte, des attentes raisonnables des utilisateurs ou des objectifs pour lesquels le produit ou service sous-jacent est offert au public. Bien qu'il s'agisse là du concept de protection de la vie privée dès la conception, le projet de loi ne contient aucune spécificité ni aucun principe de proportionnalité. Lors de l'étude article par article, ce concept n'a pas été discuté de manière suffisamment détaillée. Il serait utile d'obtenir des informations supplémentaires pour mieux comprendre la portée de cette obligation.

Recommandation (article 100)

⇒ *Nous croyons que les entreprises devraient avoir la possibilité de prendre en compte certains critères pour déterminer ce qui constitue « le plus haut niveau de confidentialité », et que ces critères devraient tenir compte des aspects opérationnels et contextuels, y compris les attentes raisonnables des personnes qui utilisent le produit ou le service. Il n'est pas toujours approprié ou nécessaire de respecter le « plus haut niveau de confidentialité », qui pourrait entraîner des mesures extrêmes et coûteuses qui ne sont pas nécessaires dans les circonstances.*

e) Technologie d'identification (article 99).

Le projet de loi crée une obligation d'« informer » les personnes de l'utilisation de technologies qui les identifient, les localisent ou les reconnaissent, ainsi que des moyens d'activer ces fonctions. Nous souhaiterions obtenir des précisions sur ce qui constitue le fait d' « informer » une personne et sur les exceptions à cette obligation. Dans la mesure où cette disposition est destinée à se concentrer sur les témoins et les pixels, il serait utile de connaître la technologie exacte envisagée et les attentes entourant cette technologie. En outre, la modification de cette section qui exige que les entreprises informent la personne des moyens disponibles pour activer les caractéristiques d'identification, de localisation ou de profilage au lieu de l'informer de la manière de désactiver ces fonctions soulève plusieurs questions, dont la plus fondamentale est de savoir comment cette modification s'applique en pratique aux technologies existantes qui sont utilisées par nos membres et qui sont essentielles à leurs activités, notamment pour aider à

prévenir la fraude. En effet, il peut être utile dans les circonstances de savoir qu'un nombre anormalement élevé de transactions ont lieu dans une localisation donnée.

Recommandations (article 99)

⇒ *Nous croyons que la divulgation dans un avis de confidentialité est suffisante pour informer les personnes des technologies d'identification.*

⇒ *Nous croyons que les activités liées à la prévention de la fraude et à la gestion des risques, par exemple, ne devraient pas être affectées négativement par les changements liés à l'activation ou à la désactivation de certaines fonctions.*

⇒ *Nous croyons que les organisations devraient être autorisées à informer les personnes qu'en utilisant un produit ou un service, elles activeront une technologie d'identification.*

f) Prise de décision automatisée (article 102)

L'article 102 du projet de loi exige que les organisations qui utilisent des moyens automatisés pour prendre des « décisions » fournissent aux personnes une explication des « raisons et des principaux facteurs et paramètres qui ont mené à ces décisions ». Cette exigence est trop large dans la mesure où elle obligera les organisations à informer les personnes de décisions automatisées qui sont peu susceptibles d'avoir des conséquences importantes, ce qui entraînera une saturation des notifications sans pour autant protéger la vie privée des individus. En outre, le niveau de détail requis sera parfois difficile à fournir sans révéler des informations sensibles ou exclusives sur l'algorithme lui-même.

Recommandations (article 102)

⇒ *Nous croyons que des lignes directrices devraient identifier le contenu, le format et la procédure acceptables pour l'explication requise par l'article 102.*

⇒ *Nous croyons que les décisions automatisées visées à l'article 102 devraient être limitées à celles qui sont susceptibles d'affecter de manière significative un individu.*

⇒ *Il est nécessaire de clarifier comment cette mesure s'appliquera dans la vie réelle, et qui est responsable lorsqu'un fournisseur de services prend une décision (par exemple, la propension à la fraude) et qui n'a pas de relation directe ou d'informations personnelles avec l'utilisateur final ou le détenteur d'une carte.*

g) Autres (commentaires généraux)

D'un point de vue général, nous croyons que le gouvernement devrait préciser comment il s'attend à ce que chaque disposition modifiée ou nouvelle de la loi sur le secteur privé soit mise en œuvre de façon pratique par les entreprises qui y sont assujetties. Plus précisément, quels changements à leurs pratiques existantes, le cas échéant, les entreprises devront-elles apporter pour se conformer à la loi – en particulier les PME qui fonctionnent souvent avec des ressources limitées. Selon l'IAPP et Ernst & Young, les entreprises ont dû dépenser en moyenne 1,8 M$ pour se conformer au GDPR en 2018.

Nous vous remercions de votre attention et de votre considération, et étant donné l'importance de ce projet de loi pour toutes les entreprises ayant des activités au Québec et pour les Québécois, l'ETA serait heureuse de recevoir toute clarification et tout détail supplémentaire afin d'aider nos membres qui travailleront avec diligence pour se conformer à leurs nouvelles obligations.

Dans l'attente, nous restons à votre disposition pour toute question relative aux présentes ou à notre industrie.

Veuillez agréer, Madame la Présidente, l'expression de nos sentiments respectueux.

Scott Talbott
Vice-président principal
Electronic Transactions Association

Cc:
Jean-Sébastien Desmeules, Secrétaire général et Directeur des affaires juridiques, Commission d'accès à l'information du Québec
Jean-Philippe Miville-Deschênes, Conseiller juridique, Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques
Jean-Christophe Lambert, Conseiller politique, cabinet du Ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels