CI– 029M
C.P. – PL 64
Protection des renseignements personnels

Commentaires de l'ABC sur le Projet de loi 64 - Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

09/28/2020

Présentés à la Commission des institutions, Assemblée nationale du Québec

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Introduction

L'Association des banquiers canadiens (« **ABC** ») se réjouit de l'opportunité de pouvoir présenter au gouvernement du Québec ses commentaires écrits exposant le point de vue du secteur bancaire sur le Projet de loi 64 du Québec - *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (« **Projet de loi 64** »).

L'ABC est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économiques du Canada. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiens à atteindre leurs objectifs financiers.

Nous saluons le leadership du gouvernement du Québec dans la présentation d'un projet de loi ayant pour objectif de mieux protéger la vie privée des Québécois.

Les consommateurs et les entreprises à travers le Canada ont bénéficié de lois provinciales et fédérales similaires en matière de protection de renseignements personnels dans le secteur privé, les exigences de chacune des juridictions n'entrant pas en conflit de manière significative. Historiquement, le Québec a toujours priorisé la protection de la vie privée et le Projet de loi 64 innove à cet égard. Nous sommes d'avis, tout comme le gouvernement québécois, que des efforts particuliers doivent être faits pour s'assurer du maintien de la confiance des citoyens envers les mesures en place pour protéger leur vie privée et la sécurité de leurs données. La confiance des consommateurs est au cœur des liens entre les banques du Québec et leurs clients; cela se traduit par l'importance que nous accordons tant à la protection de leur vie privée qu'à la gestion de leurs finances.

Dans sa forme actuelle, le Projet de loi 64 contient toutefois des exigences hautement normatives qui vont bien au-delà des principes véhiculés par les lois en matière de protection de la vie privée en vigueur dans d'autres juridictions canadiennes et à l'étranger.

Par le présent mémoire, nous souhaitons donner certains exemples où une trop grande disparité entre les régimes est susceptible de créer des défis opérationnels importants pour les entreprises et, en définitive, engendrer des effets qui vont à l'encontre des intérêts des consommateurs en augmentant les risques pour leur vie privée et en nuisant à leur expérience client.

Après avoir complété une analyse approfondie du Projet de loi 64, nous recommandons que les efforts déployés dans le cadre de ce projet soient accrus afin de favoriser une plus grande consultation des acteurs impliqués et une collaboration entre les législateurs et autres parties prenantes au niveau fédéral et entre les acteurs provinciaux. Plus particulièrement, nous recommandons aux législateurs de prendre le temps nécessaire pour évaluer les répercussions pratiques des exigences proposées en matière de protection de la vie privée sur les organisations québécoises, nationales et internationales, qui, si elles ne sont pas dûment alignées, auront des impacts négatifs non souhaitables sur les consommateurs du Québec.

Sommaire exécutif

La protection des renseignements personnels continue d'être un enjeu fondamental pour les membres de l'ABC. Toutefois, toute modification apportée aux régimes législatifs fédéraux et/ou provinciaux en matière de protection de la vie privée, qui entraîne des exigences significativement différentes d'un régime à l'autre est susceptible de causer un manque d'alignement, de coordination ou d'opérabilité. Ces changements pourraient nuire à l'innovation, frustrer les clients et générer des effets indésirables sur la sécurité des informations personnelles.

Parmi les banques membres de l'ABC, nombre d'entre elles, y compris les plus grandes banques, fournissent des produits et services financiers aux consommateurs partout au Québec et dans les autres provinces canadiennes. La *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDÉ** ») s'applique aux opérations bancaires puisque que les activités des banques relèvent de la compétence du gouvernement fédéral. Les représentations contenues aux présentes ne doivent d'aucune façon être interprétées comme constituant une reconnaissance de l'application du Projet de loi 64 aux entreprises fédérales. Les filiales provinciales des banques, comme les sociétés d'assurance ou les sociétés de placements, sont quant à elles assujetties à la législation provinciale en matière de protection de la vie privée au Québec, en Alberta et en Colombie-Britannique, puis à la LPRPDÉ dans les autres provinces.

Le fait que les institutions financières soient régies par des normes et des règlements en matière de protection de la vie privée qui sont dans leur essence similaires à l'échelle nationale permet aux consommateurs de toutes les provinces canadiennes de bénéficier d'un ensemble de protections clair et cohérent (par exemple en matière de divulgation et consentement éclairé), indépendamment des produits qu'ils détiennent, des services qu'ils reçoivent ou de leur province d'appartenance. Ceci leur permet également d'être en mesure de comprendre leurs droits en

matière de protection de la vie privée. En outre, l'alignement continu des exigences législatives en matière de protection de la vie privée entre les juridictions facilite les opérations transfrontalières, accroît la capacité à se conformer et permet aux organisations de fournir des produits et des services plus cohérents et innovants, qui profitent à tous les consommateurs.

Avec les réformes en cours au Québec, en Colombie-Britannique et plus récemment en Ontario, en plus des travaux en cours au niveau fédéral pour moderniser la LPRPDÉ, le contexte canadien de la protection de la vie privée risque de se complexifier et de ne pas être aligné. Des exigences normatives divergentes sont susceptibles de créer une expérience client frustrante, ainsi que des obstacles et une complexité accrue pour les opérations transfrontalières.

Nous soutenons une réforme qui maintient un équilibre entre les exigences en matière de protection de la vie privée pour les consommateurs et l'impact de ces nouvelles exigences sur les entreprises qui desservent ces consommateurs. Nous comprenons que le Projet de loi 64 s'inspire du *Règlement général de protection des données de l'Union européenne* (le « **RGPD** »); toutefois, il semble que les exigences prévues au Projet de loi 64 soient plus contraignantes, plus prescriptives ou autrement différentes de celles prévue au RGPD dans certaines sphères. Il y a un risque élevé que le Projet de loi 64 ait des répercussions opérationnelles importantes pour les organisations, entraînant ainsi des conséquences imprévues telles une confusion accrue des consommateurs et une diminution du choix, ce qui pourrait avoir un impact sur l'économie.

Notre mémoire cerne les enjeux liés au Projet de loi 64 déclinés en quatre sections résumées comme suit :

1. L'exigence d'un ***degré de protection équivalent pour les flux transfrontaliers des données*** sera extrêmement difficile à appliquer et onéreuse pour de nombreuses organisations. Cette exigence s'avérerait particulièrement problématique en cas d'application au secteur bancaire, notamment en raison des répercussions importantes sur les opérations nationales et internationales, les ententes d'impartition, la détection des fraudes, le risque et la prévention en matière de cybersécurité, la conformité et la prévention en matière de lutte contre le blanchiment d'argent, de même qu'au niveau de l'offre et de l'expérience des consommateurs;

2. Un certain nombre d'exigences prévues au Projet de loi 64 ***gagneraient à être clarifiées afin d'offrir une souplesse qui tient compte de la sensibilité de l'information, des risques ou encore de l'alignement aux normes nationales***. Ces

normes clarifiées pourraient également contribuer à éviter de tomber dans des exigences de conformité trop complexes ou dans de nouvelles exigences susceptibles d'entraver les opportunités d'innovation pour les organisations ayant des opérations nationales ou transfrontalières. S'attarder à ces zones de complexité permettrait d'éviter les effets indésirables susceptibles d'être involontairement imposés aux consommateurs;

3. Le Projet de loi 64 envisage la création de nouveaux ***pouvoirs de contrainte et des sanctions*** sévères incompatibles avec le degré d'incertitude lié aux exigences d'équivalence, à la nature hautement prescriptive des exigences et à l'imposition de nouvelles exigences qui mériteraient d'être davantage contextualisées et indépendantes du niveau de risque associé à une situation donnée. Considérant ce manque d'alignement entre les différentes juridictions à travers le Canada, nous recommandons la mise en place d'un système de coordination entre les juridictions pour la mise en œuvre des décisions et des sanctions; et

4. Les organisations nationales et internationales visent à favoriser l'efficacité opérationnelle à travers leurs groupes internes et les différentes juridictions, en misant sur la réduction des coûts et l'amélioration de leur offre de services aux entreprises et aux consommateurs qu'elles desservent. Ces bénéfices risquent d'être compromis par le ***manque d'alignement entre les juridictions et certains conflits*** qui pourraient résulter de l'adoption du Projet de loi 64. Pour ces organisations, le respect de certaines exigences du Projet de loi 64 pourrait être impossible à mettre en œuvre ou irréaliste. À l'inverse, selon d'autres scénarios, la conformité aux normes québécoises est susceptible de miner les effets recherchés par la législation adoptée dans d'autres juridictions.

Nous recommandons au gouvernement du Québec de continuer à travailler avec ses homologues fédéral et provinciaux à l'évaluation des conséquences, pour l'ensemble des entreprises qui ont des activités interprovinciales, des exigences proposées en matière de protection de la vie privée. Bien que ce ne soit pas l'intention du législateur, ces exigences pourraient entraîner des conséquences défavorables pour les consommateurs. Nous recommandons également au gouvernement du Québec d'envisager d'autres mesures, comme l'accroissement du rôle des autorités réglementaires dans l'éducation et la sensibilisation des individus et des organisations, l'adoption de lignes directrices claires sur les contrôles d'accès et la prévention des pertes de

données, et d'assurer un contrôle et des sanctions équitables qui soient conformes aux normes internationales et qui, en définitive, permettront davantage d'atteindre les objectifs du gouvernement du Québec.

1. Exigence d'équivalence

Nous sommes d'avis que l'exigence d'équivalence du Projet de loi 64 concernant les mouvements de données transfrontalières sera très problématique pour de nombreuses organisations et aura des conséquences négatives pour les consommateurs au Québec, tout en entrainant des défis opérationnels importants pour les banques et les autres organisations, notamment les PMEs. Les principaux enjeux liés à l'exigence d'équivalence peuvent être résumés ainsi :

- l'étendue de l'obligation n'est pas claire et crée une incertitude, alors qu'elle peut s'appliquer aux transferts internationaux et interprovinciaux de renseignements personnels, or une liste d'États équivalents n'a pas encore été publiée;

- ces normes ne sont pas alignées sur celles qui sont énoncées dans des lois comparables (par exemple, la LPRPDÉ et le RGPD) et sont sans aucun doute plus contraignantes que les exigences en matière de suffisance prévue par le RGPD (l'équivalence implique une exigence plus rigoureuse que l'adéquation), et il est très possible que certaines juridictions, comme les États-Unis et d'autres provinces canadiennes, ne satisfassent pas aux exigences en matière d'équivalence; et

- il n'y a pas de disposition claire reprenant un contenu semblable à celui des principes de responsabilité et de transparence prévus à la LPRPDÉ qui permettent aux organisations de connaître les paramètres leur permettant de transmettre des renseignements personnels aux fournisseurs de services. En particulier, contrairement au Pacte mondial des Nations Unies pour le développement durable, le Projet de loi 64 ne prévoit pas que les transferts à un État réputé non équivalent peuvent être effectués si l'organisation conserve la responsabilité et atténue le risque lié à la vie privée par des moyens contractuels.

À l'instar d'autres organisations nationales et internationales, les banques font appel à des fournisseurs de services partout au Canada et dans des juridictions étrangères (y compris des fournisseurs de services infonuagiques) pour traiter les renseignements personnels afin de fournir

les produits et les services demandés par les clients et de respecter les exigences réglementaires et juridiques applicables. Les relations entre les banques et ces fournisseurs de services sont assujetties à une réglementation rigoureuse (p. ex., la LPRPDÉ et la ligne directrice B-10 du Bureau du surintendant des institutions financières (Impartition des activités, des fonctions et des procédés commerciaux)). Toute réglementation supplémentaire est susceptible de menacer à la fois la viabilité de ces mouvements de données nécessaires et l'atteinte de l'objectif sous-jacent de la législation et de la réglementation fédérales (c.-à-d. la création d'un cadre prévisible qui permet à la fois les mouvements des données et protège les renseignements personnels des Canadiens).

La perturbation du flux de données entre provinces et à l'international aurait un impact négatif sur les consommateurs québécois et canadiens. Le traitement de données est une opération complexe. La mise en place du matériel informatique, des algorithmes et des dispositifs de sécurité nécessaires aux exigences de traitement d'une institution financière est un processus coûteux requérant d'importants investissements en capital. Certains systèmes de traitement de données pourraient tout simplement être impossibles à développer et à mettre en place à l'interne. Dans d'autres cas, le développement d'un tel système à l'interne pourrait mener à un résultat de qualité sous-optimale ou accroître la dépendance à des systèmes dont les capacités sont moindres. Si le critère d'équivalence applicable empêche les banques de communiquer avec certains fournisseurs de services, l'innovation et l'efficience des institutions bancaires pourraient en souffrir, ce qui résulterait en une offre réduite de produits et services bancaires pour les consommateurs.

De plus, le critère d'équivalence pourrait entraîner un conflit avec d'autres exigences réglementaires applicables aux banques et entraver le flux de données permettant aux différentes institutions financières de s'entraider afin de détecter, d'éliminer ou de prévenir la fraude, de gérer les menaces à la cybersécurité et d'enquêter sur les crimes financiers. Cela risque d'exacerber la fraude, la criminalité financière et les atteintes à la cybersécurité pour toutes les organisations.

Pour plus d'informations sur ces impacts potentiels pour les organisations qui opèrent dans plusieurs juridictions, veuillez-vous référer à l'annexe A.

Le critère d'équivalence est également incompatible avec les restrictions applicables au flux de données transfrontalières d'autres juridictions et avec les obligations commerciales internationales du Canada. Si le Projet de loi 64 impose effectivement le traitement et la

conservation des données localement, il pourrait alors être interprété comme un obstacle non tarifaire au commerce et, par conséquent, être incompatible avec les obligations du Canada aux termes de l'Accord Canada-États-Unis-Mexique (ACEUM), l'Accord général sur le commerce des services (AGCS) de l'Organisation mondiale du commerce, l'Accord économique et commercial global (AECG) entre le Canada et l'Union européenne, et l'Accord de partenariat transpacifique global et progressiste (PTPGP). Bien que ces ententes puissent permettre l'application des lois sur la protection de la vie privée dans le cadre des transferts transfrontaliers, les lois sur la protection de la vie privée ne peuvent imposer de restrictions excessives à ces transferts qui auraient pour effet d'annuler les avantages commerciaux découlant de ces ententes, à moins que ces restrictions ne soient absolument nécessaires pour atteindre les objectifs de ces lois.

En raison de ces conséquences potentielles pour les banques et les consommateurs décrites ci-haut, nous sommes d'avis que le critère d'équivalence prévu par le Projet de loi 64 est extrêmement complexe pour les banques, et plus particulièrement pour leurs filiales, ainsi que pour de nombreuses autres organisations nationales et internationales. Nous recommandons donc le retrait du critère d'équivalence. Cette exigence pourrait plutôt être traitée par le biais d'un mécanisme permettant aux organisations de demeurer responsables pour les renseignements personnels tout en gérant le risque qui en découle par des moyens contractuels. Les banques ainsi que de nombreuses autres organisations nationales et internationales ont besoin de prévisibilité et de flexibilité dans leur gestion des flux de données afin de leur permettre d'offrir des produits innovants et abordables aux consommateurs tout en maintenant un haut niveau de sécurité. Il est essentiel de préserver cette approche.

2. Complexification des opérations

Nous avons examiné les exigences prévues par le Projet de loi 64 et comprenons qu'elles visent à assurer une approche rigoureuse en matière de protection de la vie privée au bénéfice des consommateurs. Toutefois, à l'heure actuelle, un certain nombre d'exigences ne sont pas suffisamment claires, ne prennent pas en considération la sensibilité ou le niveau de risque, et ne correspondent pas aux définitions ou aux facteurs de risque applicables dans d'autres juridictions. Collectivement, ces exigences susciteront d'importantes difficultés opérationnelles pour les organisations de toutes tailles, ce qui aura des répercussions non anticipées sur le consentement éclairé, les choix et l'expérience offerte aux clients. Globalement, les exigences ne tiennent pas entièrement compte de la complexité du flux de données. Ces exigences pourraient donner lieu à des avis relatifs à des bris de confidentialité et des demandes de consentement

plus complexes sans offrir des choix ou des options de sécurité plus pertinentes aux individus. Cela peut entraîner des problèmes de mise en œuvre, car les exigences imposées par le Projet de loi 64 sont plus contraignantes que celles du RGPD.

Dans le tableau suivant, nous offrons des exemples où nous considérons que les exigences strictes du Projet de loi 64 diffèrent substantiellement des règles applicables en vertu du régime fédéral ou du régime applicable dans d'autres provinces ce qui, dans l'ensemble, entraînerait une complexité opérationnelle importante. De plus amples informations sur l'impact potentiel de chaque exigence sont détaillées dans l'annexe B.

Exigences prévues au Projet de loi 64	**Analyse**
1. Article 95 – Les définitions des atteintes à la protection d'un renseignement et le seuil de risque requis pour le signalement d'un incident de confidentialité	• Incohérentes avec les pratiques fédérales ou provinciales existantes en semblable matière.
2. Article 95 – Exigences pour l'évaluation des risques liés à la protection de la vie privée (par ex. l'évaluation de l'impact sur la protection de la vie privée)	• Ne prévoient aucun seuil minimal de risque, aucun niveau de sensibilité à l'information, ni aucune exigence contextuelle pour justifier une évaluation.
3. Article 95 – Portabilité des données	• Manque de clarté quant à l'étendue de la responsabilité de l'organisation. Il faut ajouter des exceptions raisonnables. • Impact potentiel pour le consommateur de l'incohérence des règles applicables dans les différentes provinces.
4. Article 99 – Profilage	• Le « profilage » n'est pas défini assez précisément et peut être interprété de façon trop large.
5. Article 100 – Plus haut niveau de confidentialité par défaut.	• Cette exigence s'applique indépendamment du degré de sensibilité de l'information et sans égard au contexte.
6. Article 102 – Les exigences de consentement	• Incohérentes avec les pratiques fédérales ou provinciales existantes en semblable matière.

Exigences prévues au Projet de loi 64	Analyse
7. Article 102 – Traitement automatisé des données dans le cadre d'un processus décisionnel	• La portée de cet article manque de clarté. Il faut prendre en considération le niveau de risque.
8. Article 102 – Définitions, incluant la dépersonnalisation.	• Les définitions manquent de clarté. Incertitude quant à la portée. • Incohérence potentielle avec le régime fédéral et ceux des autres provinces.
9. Article 109 – Définition d'accès autorisé aux employés internes	• Incohérentes avec les pratiques fédérales ou provinciales existantes en semblable matière.
10. Article 113 – Le droit à l'oubli	• La portée manque de clarté. Nécessite l'ajout d'exceptions raisonnables. • Incohérence potentielle avec le régime fédéral et ceux des autres provinces.

3. Contraintes et sanctions

Alors que les mesures de mise en œuvre et de sanction prévues par les différentes lois sur la protection de la vie privée à l'international font présentement l'objet de révision et de réforme, nous soulignons la nécessité de mettre en place certaines garanties assurant l'équité procédurale. Il faut notamment assurer que les organisations faisant l'objet de mesures de contrôle en vertu de la loi aient le droit de comprendre les allégations les visant, d'être entendues, d'être représentées par un avocat, d'avoir des motifs écrits, une audience impartiale et une procédure d'appel.

Nous suggérons également que les régimes de contrôle et de sanctions qui tiennent compte des scénarios suivants

- Il est possible qu'un seul incident lié à la protection de la vie privée entraine, pour une même organisation des amendes multiples de plusieurs organismes canadiens de réglementation. Ultimement, le montant de ces amendes cumulées pourrait dépasser le montant envisagé par chacune des juridictions concernées.

- S’il existe des différences importantes entre les exigences applicables d’une juridiction à l’autre, un seul incident lié à la protection de la vie privée pourrait générer pour une même organisation, une série de conclusions ou décisions contradictoires. Ces conclusions ou décisions pourraient être difficiles, voire même impossibles à mettre en œuvre selon les des opérations commerciales de l’organisation concernée. Cela pourrait aussi entraîner des sanctions additionnelles par une ou plusieurs juridictions si les ordonnances ne sont pas respectées par la suite.

- Un incident survenant au sein d'une filiale assujettie à la réglementation provinciale pourrait amener un organisme de réglementation provincial à imposer une pénalité à une société mère de juridiction fédérale (4 % des revenus mondiaux, le double en cas de récidive).

En outre, étant donné l'incertitude quant aux juridictions qui peuvent être considérées comme équivalentes pour les transferts de données transfrontaliers (décrite dans la section 1) et le manque de clarté, de proportionnalité et de d’alignement des définitions et des exigences (décrits dans la section 2), les organisations seront confrontées à une incertitude considérable dans la gestion de la conformité et des impacts opérationnels résultant des exigences du Projet de loi 64. Comme nous le soulignons plus loin dans la section 4, les impacts du projet de loi sur les organisations nationales et internationales n'ont pas été entièrement évalués. Par ailleurs, il faudra peut-être des années aux grandes organisations pour être pleinement conformes étant donné l'ampleur des changements nécessaires pour intégrer les exigences proposées dans les systèmes ou les processus, ou pour mettre fin aux engagements contractuels à long terme avec les fournisseurs de services existants et conclure de nouvelles ententes.

Compte tenu de ce niveau d'incertitude et du degré potentiel de changement requis, nous estimons que les amendes et pénalités maximales prévues par le Projet de loi 64 sont déraisonnables.

De plus, nous recommandons qu'il y ait une coordination multi juridictionnelle formelle des conclusions ou des décisions rendues et des sanctions émises par les organismes de réglementation de la protection de la vie privée. Cela s’est déjà fait de manière informelle lors d'enquêtes et de conclusions précédentes impliquant des organismes de réglementation fédéraux et provinciaux de la protection de la vie privée. Les régimes de mise en œuvre modernes sont encore assez récents et peu de sanctions significatives ont été imposées, il est donc difficile

de s'inspirer des meilleures pratiques dans ce domaine. Dans le modèle du RGPD, le lieu du principal établissement de l'organisation détermine généralement quel organisme de réglementation assurera la mise en œuvre des règles et l'application des sanctions appropriées. Cette approche n'est peut-être pas applicable dans un contexte canadien où il y a eu récemment une coopération plus étendue entre les commissaires fédéral et provinciaux à la protection de la vie privée pour les enquêtes et les ordonnances. Une organisation ayant des activités à travers le Canada pourrait faire l'objet de sanctions imposées par plusieurs provinces et/ou le fédéral en raison d'un seul et même cas de non-conformité (par exemple, une brèche dans la protection des données qui touche les résidents de plusieurs provinces, ou un produit ou service national qui fait l'objet d'une enquête ou d'une plainte en matière de protection de la vie privée). Un modèle canadien pourrait prévoir que des sanctions cumulatives imposées par plusieurs juridictions ne doivent pas excéder la limite maximale d'une juridiction en particulier ou encore prévoir que la sanction est calculée au prorata de la taille de la juridiction. Ces limites devraient également prendre en considération l'étendue de l'infraction lorsque l'on examine les relations entre une compagnie mère et sa filiale.

4. Répercussions transjuridictionnelles

Tel que mentionné au début du présent mémoire, les consommateurs ont historiquement profité de l'uniformisation et l'alignement des normes en matière de protection des renseignements personnels à travers les juridictions canadiennes qui permettent:

- la disponibilité d'ensembles de protections cohérentes et de qualité, sans tenir compte du produit ou du service ou du lieu de résidence des consommateurs;
- d'éviter les exigences divergentes en matière de divulgation et de consentement; et
- aux consommateurs de comprendre aisément leurs droits en matière de protection des renseignements personnels.

L'uniformisation a également facilité la conformité et l'efficacité opérationnelle parmi les groupes bancaires, malgré le fait que leurs diverses entités soient assujetties à des lois fédérales ou provinciales différentes en matière de protection des renseignements personnels. À titre d'exemple, les sociétés mères et leurs filiales peuvent bénéficier collectivement de ce processus, systèmes et relations avec des fournisseurs de services, tant au niveau national qu'international,

afin de réaliser des économies d'échelle et faciliter la conformité. Cela est courant dans les organisations nationales et internationales.

Les modifications proposées par le Projet de loi 64 pourraient nuire à l'uniformisation des normes en matière de protection des renseignements personnels, qui jusqu'à présent aura largement profité tant aux organisations qu'aux consommateurs. Plus précisément, les répercussions potentielles du Projet de loi 64 sur les organisations où les normes peuvent s'appliquer de façon extraterritoriale ou extra-juridictionnelle ne semblent pas avoir été pleinement envisagées.

Présentement, la *Loi sur la protection des renseignements personnels dans le secteur privé* est jugée essentiellement semblable à la LPRPDÉ et aux autres lois provinciales sur la protection des renseignements personnels, sans conflit majeur.

Toutefois, nous croyons que les nombreuses exigences normatives et plus rigoureuses du Projet de loi 64 se distinguent considérablement des modifications proposées à la LPRPDÉ ou des normes concernant la protection des renseignements personnels établies dans d'autres provinces. Pour les organisations, cela entraînera des répercussions importantes sur leurs activités existantes et, dans certains cas, rendra impossible sur le plan opérationnel certaines activités (p. ex., pour certains processus spécialisés, ententes d'impartition et normes réglementaires). Ces défis ont été détaillés ci-dessus (sections 1, 2 et 3). Par conséquent, si les éléments contraignants proposés par le projet de loi étaient appliqués aux entreprises et aux banques, celles-ci pourraient se retrouver dans une situation imprévisible et complexe. Parmi les conséquences négatives potentielles :

1. L'assujettissement des entreprises à d'importantes pénalités (qui pourraient représenter 4 % de leurs revenus mondiaux, ou même le double pour les récidivistes) alors qu'elles ne sont pas en mesure de se conformer à certaines exigences normatives du Projet de loi 64; et/ou

1. Dans certains cas, la séparation ou la ségrégation des normes pour certains processus ou systèmes partagés entre les entités fédérales et provinciales d'un même groupe seraient difficilement envisageables et réalisables, notamment dans le secteur bancaire. Se conformer efficacement aux modifications proposées par le Projet de loi 64, dans le cadre de toutes les opérations d'une entreprise ou d'une institution bancaire, entraînerait des résultats discordants car ses exigences ne correspondront pas aux attentes de d'autres juridictions.

Conclusion

En conclusion, l'ABC soutient les efforts déployés par le Gouvernement du Québec visant l'amélioration des protections en matière de renseignements personnels accordées aux consommateurs. Toutefois, tel que rédigé, le Projet de loi 64 risque d'entraîner un manque de cohésion ou de coordination des exigences en matière de protection des renseignements personnels entre les juridictions canadiennes fédérale et provinciales et de créer une confusion qui nuirait aux intérêts des consommateurs et entreprises du Québec.

Comme nous l'avons souligné tout au long de notre mémoire, le Projet de loi 64 imposerait des restrictions plus contraignantes aux entreprises québécoises que la LPRPDÉ et le RGPD. Ces restrictions pourraient entraîner pour les consommateurs et les entreprises des conséquences négatives qui ne semblent pas avoir été évaluées. Il n'y a aucune démonstration ni certitude que la mise en œuvre du Projet de loi 64 et les avantages en matière de protection des renseignements personnels qui en découleraient soient supérieurs à ceux qui ont suivi l'adoption du RGPD. En fait, les effets négatifs du Projet de loi 64 pourraient d'ailleurs être plus marqués que ce qui ressort de l'expérience vécue depuis l'entrée en vigueur du RGPD. L'exigence d'équivalence contenue dans le Projet de loi 64 est plus restrictive que l'exigence d'adéquation du RGPD et pourrait nuire à la circulation des données. Ses exigences en matière de consentement pourraient entraîner une exaspération des consommateurs à cet égard et un manque de consentements significatifs. Dans l'ensemble, nous croyons que l'ensemble des normes prévues dans le Projet de loi 64 entraînera d'importantes complexités opérationnelles pour les organisations de toutes tailles, ce qui aura des répercussions sur les gammes de produits et de services offerts ainsi que les choix et l'expérience des consommateurs.

Nous suggérons que le gouvernement du Québec utilise son leadership pour collaborer avec ses homologues fédéral et provinciaux et les acteurs du milieu afin d'évaluer les répercussions opérationnelles globales qu'auront les réformes proposées en matière de protection des renseignements personnels, y compris les répercussions sur les organisations locales, nationales et internationales. Bien que nous soutenons le fait que le Projet de loi 64 priorise les intérêts des consommateurs, l'augmentation considérable de la complexité et de la charge opérationnelle pour les entreprises ne peut être ignorée, car nous estimons que cela entraînera des répercussions défavorables et indésirables.

À notre avis, les éléments qui suivent permettraient de mieux répondre aux objectifs sous-jacents du Projet de loi 64 tout en permettant aux gouvernements du Québec, du Canada et aux autres gouvernements provinciaux de faire progresser d'autres objectifs de politique publique :

1. Continuer de renforcer et de mettre l'accent sur le concept de responsabilité des entreprises quant à leurs pratiques de protection des renseignements personnels, de manière cohérente avec les normes fédérales en matière de responsabilité;

2. Introduire le concept de proportionnalité et d'équilibre dans l'ensemble du projet de loi, répondant ainsi aux enjeux liés à la charte opérationnelle;

3. Rechercher une cohérence dans les définitions, les seuils de risque et les exigences de consentement à travers le Canada;

4. Augmenter la sensibilisation en matière de protection des renseignements personnels et l'éducation offerte

    - par les organismes de réglementation quant aux obligations des organisations quant à leurs obligations; et

    - par les organisations à leurs employés;

5. Adopter des lignes directrices pour promouvoir la mise en place de mesures de contrôle d'accès appropriées ainsi que la surveillance et la prévention des pertes de données; et

6. Mettre en œuvre des pouvoirs de mise en œuvre et des pénalités équitables pour favoriser la conformité (voir la section 4).

Il nous fera plaisir de répondre à toutes questions relativement aux analyses et avis contenus dans ce document, et d'en discuter plus amplement, à votre convenance, tout au long du processus en cours.

Annexe A - Exemples de répercussions des exigences d'équivalence proposées :

Pour compléter la section 1 du présent mémoire, cette annexe fournit des précisions supplémentaires sur certaines répercussions qui pourraient découler des exigences d'équivalence du Projet de loi 64, puisqu'une incertitude demeure quant aux États (au Canada ou à l'extérieur du Canada) qui seraient considérés comme équivalents. Plusieurs de ces répercussions sont pertinentes pour d'autres organisations nationales ou internationales.

Répercussions réglementaires :

En plus de la législation en matière de protection des renseignements personnels, les banques sont fortement réglementées et sont soumises à des obligations réglementaires dans plusieurs juridictions qui exigent que certains renseignements personnels soient communiqués à des organismes de réglementation situés dans d'autres provinces ou pays dans certaines circonstances. Ces obligations réglementaires peuvent être incompatibles avec le respect de l'exigence d'équivalence prévue au Projet de loi 64 si un organisme de réglementation se trouve dans un État qui n'est pas considéré comme équivalent.

Par exemple, selon le *Règlement sur le recyclage des produits de la criminalité et le financement des activités terroristes*, les filiales de gestion de patrimoine sont tenues de signaler à CANAFE (situé en Ontario) toutes opérations suspectes et autres opérations déterminées, incluant la communication de renseignements personnels. Certaines de ces obligations réglementaires sont souvent reliées aux obligations internationales du Canada et, éventuellement, aux normes internationales, p. ex., avec la *Financial Industry Regulatory Authority* (FINRA) aux États-Unis. Étant donné que les activités de blanchiment d'argent ne sont pas limitées territorialement, le Québec et le Canada doivent être en mesure de lutter contre le blanchiment d'argent et le financement des activités terroristes à l'échelle nationale et internationale afin de respecter leurs obligations et engagements réglementaires internationaux en matière de lutte contre la criminalité financière transnationale.

De plus, certains fournisseurs de services internationaux participent au traitement et à l'exécution des obligations réglementaires (p. ex., pour le contrôle des sanctions, les exigences relatives à la connaissance et l'identification de ses clients et le contrôle et la surveillance des transactions). Dans certains cas, il peut être impossible de migrer ces systèmes et/ou processus, étant donné qu'ils peuvent faire l'objet de contrats avec des fournisseurs de services de classe mondiale dans

certains domaines hautement spécialisés et limités, ou qu'ils peuvent être centralisés avec une société mère dans un autre territoire.

Enfin, les consommateurs ont de plus en plus, des besoins à l'échelle mondiale. Par conséquent, les banques internationales facilitent leur accès aux services. Toutefois, cela implique la nécessité de fournir certains renseignements personnels ou de se conformer aux réglementations contre le blanchiment en vigueur dans d'autres pays où l'organisation n'exerce même pas ses activités. C'est le cas par exemple lors d'un transfert de fonds transfrontalier.

Répercussions sur la détection et la prévention de la fraude et des autres crimes financiers :

La fraude et d'autres crimes financiers ont des répercussions importantes sur les consommateurs dans toutes les provinces. La criminalité financière est vaste, incluant la fraude, le vol de données/de renseignements personnels, le blanchiment d'argent, le financement d'activités terroristes, la cybercriminalité, les cambriolages, le harcèlement/les agressions physiques et la traite de personnes. Il est essentiel que nos membres soient en mesure de détecter, prévenir et combattre la criminalité financière, car ces efforts contribuent à maintenir la sécurité et l'intégrité du système financier canadien et de son infrastructure ainsi qu'à protéger les clients (p. ex., contre la perte financière, le vol d'identité ou la perturbation de leurs activités financières).

Une grande partie des crimes financiers se produisent au-delà des frontières provinciales, à l'échelle nationale et internationale, et à travers plusieurs secteurs de l'industrie. Pour combattre efficacement les crimes financiers, il faut analyser les renseignements personnels en temps opportun dans toutes les régions afin d'exploiter l'information (p. ex., des indicateurs de compromis ou des tendances clés); sans ces informations, ceux qui constituent cette menace continueront à commettre des crimes financiers et à échapper à la justice.

Si les informations sur la fraude et la criminalité financière au Québec ne peuvent être partagées entre les territoires en raison de l'exigence d'équivalence du Projet de loi 64, nos membres ne pourront pas détecter et prévenir efficacement la fraude nationale ou internationale, ce qui affectera non seulement nos propres membres, mais d'autres au sein du système bancaire national et international qui comptent sur ces informations pour protéger leurs clients et s'attaquer à ceux qui constituent cette menace. Il en va de même pour les autres secteurs exposés à la menace d'une grave criminalité financière.

Répercussions sur la cybersécurité :

Les restrictions imposées à la circulation des données limiteront le partage d'informations essentielles, réduiront les options offertes pour les services de cybersécurité et accentueront les risques liés à la cybersécurité. Par exemple, les organisations de toutes tailles font affaire avec des fournisseurs de services « cloud » (p. ex., Amazon Web Services et Microsoft Azure) pour plusieurs raisons telles leur capacité de stockage et de traitement et, surtout, leur offre de meilleures protections de cybersécurité qu'elles ne peuvent pas reproduire à l'interne. Dans certains cas, les organismes peuvent même crypter les données avant que celles-ci ne soient envoyées vers le « cloud », les données étant ainsi inaccessibles (y compris pour le fournisseur de services ou les organismes gouvernementaux situés dans la juridiction du fournisseur de services).

Si certains services « cloud » ne peuvent être considérés (si leurs serveurs sont situés dans d'autres juridictions qui ne sont pas considérées comme équivalentes), ou si un ou plusieurs fournisseurs clés se retirent du marché québécois en raison de leurs propres préoccupations en matière de responsabilité, les risques de cybersécurité pourraient augmenter, ce qui est particulièrement préoccupant pour les infrastructures financières essentielles qui assurent la protection des avoirs financiers des clients (comme un compte d'investissement). En outre, forcer les organisations à regrouper leurs risques en stockant toutes leurs données dans une ou quelques juridictions amplifie non seulement les cyber-risques, mais également les risques liés à la fiabilité et à la disponibilité des systèmes. Cette préoccupation a été étudiée par le Forum Économique Mondial, qui a évalué les conséquences de la localisation des données et a identifié les problèmes de sécurité des données et les cyber-risques en raison d'un manque de diversification.[1]

[1] Forum économique mondial – « A Roadmap for Cross Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy », juin 2020 https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy

Annexe B- Analyse des exigences provinciales particulières :

Pour compléter la section 2 du présent document, la présente annexe donne des exemples d'exigences spécifiques du Projet de loi 64 qui pourraient bénéficier d'une plus grande clarté, uniformisation et/ ou cohérence avec les normes correspondantes des autres juridictions. Collectivement, ces exigences peuvent entraîner des difficultés d'opération d'un territoire à l'autre et des répercussions défavorables non souhaitées pour les consommateurs.

1. Les ***définitions des violations et le seuil de risque requis pour le signalement*** de manquements énoncées à l'article 95 du Projet de loi 64 ne sont pas conformes aux autres pratiques fédérales ou provinciales existantes. La définition d'« incident de confidentialité » énoncée au Projet de loi 64 comprend l'utilisation non autorisée de renseignements personnels (par exemple, la commercialisation par inadvertance sans consentement). Le « risque de préjudice sérieux » du Projet de loi 64 ne fait pas l'objet d'une évaluation contextuelle de la probabilité énoncée dans la LPRPDÉ et dans la *Loi sur la protection des renseignements personnels* de l'Alberta, c'est-à-dire une évaluation de la probabilité d'un risque réel de préjudice grave. Cela pose un problème pour les organisations ayant des opérations centralisées et nationales de service à la clientèle, car les différents déclencheurs de notification et de signalement peuvent entraîner confusion et erreur humaine.

2. L'article 95 du Projet de loi 64 ne prévoit aucun seuil minimal de risque, aucun niveau de sensibilité à l'information ni aucune exigence contextuelle pour exiger une évaluation des risques liés à la protection de la vie privée (c.-à-d., ***l'évaluation*** de l'impact sur la protection de la vie privée) et exige que chaque évaluation soit effectuée après avoir consulté la personne responsable de la protection des renseignements personnels (p. ex., chef de la protection de la protection de la vie privée). Cette exigence n'est pas réalisable, surtout dans les grandes organisations qui peuvent mener de front des milliers de projets, dont plusieurs comportent un risque minimal en matière de protection de la vie privée.

3. L'article 95 du Projet de loi 64 énonce une obligation de s'assurer de la portabilité des données soit la possibilité de communiquer à la personne concernée dans un format technologique structuré et couramment utilisé les renseignements personnels informatisés recueillis auprès d'elle. Les commentateurs en matière de sécurité ont

noté que ce droit est associé à des risques comme le vol ou la divulgation de données centralisées pour le partage ou le transfert à une personne qui n'est pas la bonne.[2]

Cette exigence devrait être adaptée aux normes sectorielles et aux normes nationales applicables. Le Projet de loi 64 devrait préciser que cette communication d'informations ne devrait pas être assujettie à des exigences d'évaluation de l'impact sur la vie privée ni à des renseignements commerciaux confidentiels. Si le client exige une communication de renseignements personnels, il doit être clair que l'organisme qui publie les renseignements n'est plus responsable de la confidentialité et de la sécurité des renseignements. Ce droit à la portabilité des données peut entraîner un risque accru pour la sécurité des données pour les clients s'ils choisissent de transmettre leurs données à une organisation dont les garanties de sécurité sont moindres ou qui peuvent utiliser leurs informations d'une manière différente; il incomberait au client de s'assurer qu'il soit à l'aise avec les politiques et pratiques de confidentialité des organismes qui recevront les renseignements les concernant.

4. Dans l'article 99 du Projet de loi 64, le « ***profilage*** » n'est pas suffisamment défini et peut être interprété de façon trop large. Le concept et l'exigence de divulgation du profilage et la possibilité d'une option de désactivation semblent convenir pour traiter le profilage en ligne à des fins publicitaires par des annonceurs tiers-parties. Nous estimons qu'il convient de clarifier le concept afin de définir des limites quant à son applicabilité; par exemple, dans le RGPD, le "profilage" se limite explicitement aux activités en ligne pour prédire les préférences, les comportements et les attitudes. La définition ne devrait pas s'appliquer à des activités commerciales bénéfiques pour les consommateurs, par exemple, des analyses internes portant sur la clientèle de l'entreprise dans le but de développer et d'offrir des produits et des services ou de mieux servir les clients.

5. L'article 100 du Projet de loi 64 précise que, lorsque des renseignements personnels sont recueillis lors de l'offre d'un produit ou d'un service technologique, les paramètres du produit ou du service doivent offrir ***le plus haut niveau de confidentialité par défaut***. Il y a un manque de clarté quant à la portée de cette exigence (p. ex., interface

[2] Institut national de la sécurité, Règlement sur la protection de la vie privée et conséquences imprévues pour la sécurité, 8-9 (2019).

client seulement, produit ou service de bout en bout, garanties et contrôles d'accès uniquement?) Cette exigence s'applique également indépendamment du degré de sensibilité de l'information. Un sondage en ligne recueillant de l'information non sensible doit-il être assujetti au même niveau de confidentialité que les mots de passe, qui sont masqués lors de l'entrée, chiffrés dans les systèmes et non accessibles aux employés? Le respect de cette norme n'est pas possible pour la plupart des cas; par exemple, dans de nombreux cas, les clients doivent pouvoir examiner ce qu'ils ont saisi dans une demande en ligne avant de soumettre, et les conseillers doivent avoir accès aux informations sur les clients pour qu'ils puissent offrir un service et conseiller leurs clients. Les activités de nos membres assujettis aux lois provinciales pourraient en souffrir lourdement si tous les produits et services en ligne ou mobiles existants et futurs devaient être assujettis à une plus grande confidentialité par défaut.

6. ***Les exigences de consentement*** énoncées à l'article 102 du Projet de loi 64 diffèrent considérablement de celles de la LPRPDÉ. Elles augmenteront considérablement la documentation que les clients doivent examiner et auront pour effet d'empêcher des utilisations commerciales légitimes. Plus particulièrement, le consentement doit être demandé pour chaque fin spécifique pour laquelle il est donné. Le consentement doit être recueilli distinctement des autres renseignements fournis au client (p. ex., séparément du formulaire de demande de services). Un consentement distinct pour chaque fin compliquerait les politiques en matière de protection de la vie privée, omettrait de reconnaître la complexité des flux de données et serait contraire aux meilleures pratiques qui visent à simplifier le consentement et à offrir aux particuliers des choix plus significatifs.

   En outre, le Projet de loi 64 exige que le consentement à la collecte et à l'utilisation d'informations sensibles soit expressément donné et que les utilisations autorisées sans consentement soient limitées. Il n'est pas certain que les pratiques commerciales raisonnables suivantes pourraient être mises en œuvre sans le consentement :

   - administrer les processus de destruction des dossiers;
   - la création et l'utilisation d'informations anonymes par l'entité qui les a recueillies;
   - la formation des employés, lorsque la dépersonnalisation n'est pas efficace (formation au service à la clientèle);
   - comprendre les besoins des clients et concevoir, développer ou améliorer des produits et des services;

- l'évaluation de la faisabilité d'un nouveau produit ou d'une nouvelle offre de services (p. ex., la démonstration de faisabilité et les projets pilotes);
- gérer les risques, les erreurs ou améliorer la qualité de l'information en permettant le recoupement des ensembles de données; et
- respecter les exigences d'autoréglementation et la réglementation.

Les exigences du Projet de loi 64 en matière de consentement peuvent surcharger les consommateurs, décourager la divulgation en toute transparence des renseignements personnels et compromettre l'utilité et la pertinence du consentement, ce qui peut entraîner une certaine exaspération de la clientèle quant aux politiques sur la protection de la vie privée.

7. L'article 102 du Projet de loi 64 énonce les droits et obligations relatifs au traitement automatisé des données dans le cadre d'un processus décisionnel. Plus particulièrement, un préavis de traitement automatique aux fins de la prise de décisions est exigé. De plus, sur demande, l'identification des renseignements personnels qui ont été utilisés aux fins de la prise de décisions automatisées, les motifs et les paramètres qui ont mené à la décision doivent être communiquée à la personne concernée. Par ailleurs, la personne concernée doit être informée de son droit de rectification des renseignements personnels inexacts utilisés pour la prise de décision. Il n'est pas certain que cette exigence vise la prise de décisions fondées sur l'intelligence artificielle (IA) en plus de la prise de décisions non liées à l'IA. Cette exigence ne tient pas compte de l'importance ni du risque lié aux décisions. Bien que le Projet de loi 64 ait un objectif de transparence sans avoir d'incidence sur l'information[3] exclusive et confidentielle d'une organisation, l'ambiguïté de cette exigence continue d'entraîner un risque que ces obligations obligent les sociétés à divulguer une forme quelconque d'information privilégiée sur leurs stratégies d'affaires, leurs activités ou les technologies qu'elles utilisent (y compris l'outil ou les algorithmes de prise de décision qu'elles utilisent), ce qui ne favoriserait pas l'innovation. En outre, l'IA et les analyses de données sont des moyens de défense essentiels contre les acteurs malveillants pour faire face aux attaques à la

[3] Analyse d'impact règlementaire

https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/AIR_PL_PRP.pdf?1596739519

cybersécurité, lutter contre le blanchiment d'argent et prévenir la fraude. Qu'on le veuille ou non, une telle ambiguïté aurait pour conséquence d'enrayer la capacité des organismes à détecter des comportements ou des transits d'information anormaux et ce, au détriment des consommateurs du Québec et du bien public.

8. La définition de renseignement « dépersonnalisé » énoncée à l'article 102 du Projet de loi 64 et la définition de renseignement « anonymisé » énoncée à l'article 111 ne tiennent pas compte du fait qu'il existe un éventail d'identifiants allant de l'information qui ne permet pas la réidentification des renseignements qui concernent directement un individu et permettent de l'identifier. De plus, le Projet de loi 64 ne permet que des utilisations très limitées de cette information soit à des fins d'étude ou de recherche ou pour la production de statistiques ou encore, comme alternative à la destruction lorsque les fins pour lesquelles les renseignements ont été recueillis sont accomplies.

Les niveaux de protection de la vie privée devraient varier et tenir compte, pour chaque renseignement, du degré de facilité avec lequel il permet d'établir l'identité d'une personne (p. ex., au niveau des exigences liées au consentement, aux fins raisonnables ou aux garanties). Par exemple, la législation devrait prévoir des règles pour la création, l'utilisation et la communication d'informations « pseudonymisées », dans lesquelles les identifiants sont remplacés afin que les données puissent être utilisées et partagées sans qu'il soit possible de faire la corrélation entre les données et un individu particulier. Les données pseudonymisées sont utiles à des fins d'innovation et de développement. Si l'anonymisation est irréversible et que l'organisation recevant des données n'a pas la clé secrète nécessaire pour identifier à nouveau un individu une fois que les données ont été anonymisées et ne peut y accéder, ces données doivent être entièrement exclues des exigences en matière de confidentialité, car il ne s'agit pas de renseignements personnels.

De plus, si le spectre et les définitions de l'identifiabilité du Projet de loi 64 diffèrent des définitions définies dans les modifications proposées à la LPRPDÉ ou d'autres lois provinciales, les organisations nationales et internationales auront de grandes difficultés à mettre en œuvre des exigences en matière de protection de la vie privée qui s'appuient sur ces définitions. Conséquemment, cela peut également entraîner des risques pour les consommateurs si les exigences en matière de protection diffèrent d'un territoire à l'autre.

9. ***L'accès autorisé par les employés internes très limité*** entraînera une obligation de divulgation dans les situations où il n'est pas raisonnable de croire qu'il existe un risque réel de préjudice important pour une personne. Contrairement à ce qui prévaut dans d'autres territoires canadiens, au Québec, une telle déclaration ne sera pas sujette à une analyse préliminaire. L'article 109 du Projet de loi 64 stipule que « les employés ou mandataires autorisés ne peuvent avoir accès aux renseignements personnels sans le consentement de la personne concernée que si ces renseignements sont nécessaires à l'exercice de leurs fonctions ». Cela pourrait être interprété comme le fait que si un employé recherche Monsieur/Madame X dans le système client, mais qu'il affiche à l'écran le mauvais Monsieur/Madame X, une violation de confidentialité devrait être enregistrée dans le registre des infractions de la société. De même, l'obligation de consigner dans le registre des infractions de la société pourrait être déclenchée si un employé du même département voyait apparaître à l'écran d'un autre employé des renseignements personnels d'un client. Il n'est pas non plus certain que l'utilisation de renseignements personnels sans consentement à des fins de formation soit autorisée (c'est-à-dire dans des situations de formation où l'utilisation de données anonymes ou créées par algorithme ne serait pas efficace, comme la formation au service à la clientèle).

10. L'article 113 du Projet de loi 64 fait référence à ce que l'on appelle communément ***le droit à l'oubli*** - l'obligation de cesser la diffusion ou de désindexer, dans certaines circonstances, les hyperliens rattachés à des renseignements personnels. L'objectif de cette exigence semble bien adapté à l'échange de renseignements personnels en ligne (p. ex., par l'intermédiaire de moteurs de recherche). Il n'est pas certain que l'exercice de ce droit n'affectera pas les systèmes organisationnels internes ou la capacité de conserver des renseignements à des fins légitimes. Par exemple, cette exigence ne tient pas compte du fait qu'il peut exister des exigences juridiques ou réglementaires auxquelles les organismes doivent satisfaire (p. ex., le dépôt de déclarations d'opérations suspectes auprès des organismes de réglementation). De plus, comme la signification du terme « diffusion » n'est pas claire, il est possible que ce droit s'applique par inadvertance au-delà du partage de renseignements personnels en ligne et entrave ainsi des opérations commerciales raisonnables et légitimes (comme les initiatives de prévention de la fraude impliquant des tiers fournisseurs de services).