

# MISE EN ŒUVRE DE LA PORTABILITÉ DES DONNÉES : LEÇONS SERVANT À L'ÉLABORATION D'UN MODÈLE CANADIEN



**À PROPOS DE COMPTABLES PROFESSIONNELS AGRÉÉS DU CANADA**

Comptables professionnels agréés du Canada (CPA Canada) travaille en collaboration avec les ordres de CPA des provinces, des territoires et des Bermudes, et représente la profession comptable canadienne sur les scènes nationale et internationale. La profession canadienne peut ainsi faire la promotion de pratiques exemplaires, favorables aux entreprises et à la société en général, et préparer ses membres aux défis posés par un contexte en évolution constante, marqué par des changements sans précédent. Forte de plus de 220 000 membres, CPA Canada est l'une des plus grandes organisations comptables nationales au monde. [cpacanada.ca](http://cpacanada.ca)

La version électronique de ce document est disponible sur le site [cpacanada.ca](http://cpacanada.ca).

© 2021 Comptables professionnels agréés du Canada

Tous droits réservés. Cette publication est protégée par des droits d'auteur et ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise de quelque manière que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode) sans autorisation écrite préalable.

# Table des matières

<b>Introduction</b> .....	<b>4</b>
<b>La portabilité des données : qu'est-ce que c'est, et quelle est son importance?</b> .....	<b>8</b>
Portabilité des données ou mobilité des données : quelle est la différence? ...	11
<b>Cadres relatifs à la portabilité des données ailleurs dans le monde</b> .....	<b>12</b>
Approches d'autres pays .....	12
Prise de mesures par les provinces canadiennes.....	14
La Loi sur la protection de la vie privée des consommateurs (LPVPC) comparée à d'autres cadres de protection des données personnelles.....	15
<b>Mise en œuvre de la portabilité des données : enjeux et défis</b> .....	<b>17</b>
Champ d'application de la portabilité des données.....	17
Processus d'authentification du client.....	19
Allègement du fardeau du traitement administratif pour les entreprises.....	21
Interfaces de protocole d'application et plateformes interopérables .....	24
Attestation de la compétence des destinataires des données transférées.....	26
<b>Conclusion</b> .....	<b>28</b>

# Introduction

À l'heure où l'économie numérique continue son expansion, vu l'émergence de préoccupations relatives au droit à la vie privée, les pays du monde entier sont amenés à renforcer leurs lois sur la confidentialité des données et à accorder aux consommateurs davantage de contrôle sur leurs données personnelles. En même temps, les progrès de la technologie et l'augmentation constante du volume de données sur les consommateurs ouvrent de nouvelles possibilités aux entreprises qui sauront les exploiter.

Au Canada, le gouvernement fédéral a déposé un projet de loi sur la réforme de la protection de la vie privée qui vise à moderniser et à renforcer la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Par le projet de loi C 11, également connu sous le nom de *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, on propose de remplacer la LPRPDE par la nouvelle *Loi sur la protection de la vie privée des consommateurs* (LPVPC), qui donnerait aux consommateurs canadiens plus de pouvoir sur leurs données personnelles conservées par les organisations. La nouvelle loi comprend de nouveaux droits relatifs à l'accès, à la correction et à la suppression des données personnelles (que certains appellent les « droits des personnes concernées »).

Ces droits comprennent également un nouveau droit à la mobilité des données qui permettra aux consommateurs canadiens de demander aux organisations de transférer leurs données personnelles à une autre organisation pour qu'elles soient réutilisées. Ce droit devrait élargir le choix des consommateurs et stimuler l'innovation commerciale en leur donnant plus de contrôle sur les informations qu'ils communiquent aux entreprises. La mobilité des données a pour but d'aider les consommateurs à éviter de se retrouver pris dans une relation avec une entreprise numérique – qu'il s'agisse d'une banque, d'un service de diffusion en continu ou d'une plateforme de médias sociaux – parce qu'il est difficile de changer de fournisseur de services.

L'idée est de donner plus de choix aux consommateurs, tout en uniformisant les règles du jeu pour les entreprises en démarrage innovantes et les autres entreprises, grâce à l'accès à une quantité accrue de données qu'elles peuvent utiliser afin d'améliorer leurs services et de créer de nouvelles offres.

En même temps, ce virage pourrait imposer des obligations importantes aux entreprises qui auront à traiter les demandes de portabilité des données, que ce soit pour transférer les données, pour les recevoir, ou pour accomplir ces deux fonctions. Elles devront probablement renforcer leurs systèmes de collecte et de stockage des données, rehausser leurs mesures de cybersécurité et de protection de la vie privée, et élaborer des processus et des protocoles pour gérer ces demandes.

L'étendue de ces obligations reste cependant à déterminer, car les règlements détaillés relatifs à la mise en œuvre du changement ne seront élaborés qu'après l'adoption des textes législatifs.

Comptables professionnels agréés du Canada (CPA Canada) s'attend à ce que les comptables professionnels, en toute probabilité, jouent un rôle central pour faciliter la conception, la mise en place, la gestion et la certification des processus de conformité, au sein de leur propre organisation ou de celle de leurs clients. Nous croyons qu'il est important, dans l'intérêt public, de s'assurer que les règlements d'application établissent un juste équilibre, pour élargir les choix des consommateurs et encourager l'innovation, tout en réduisant au minimum les coûts supplémentaires et les autres fardeaux qui pourraient nuire à la compétitivité des entreprises canadiennes.



Nous croyons également qu'au fur et à mesure que se fera le travail de conception de ces règlements, le gouvernement fédéral bénéficiera des leçons que livre l'expérience d'autres pays ayant accordé des droits semblables à leurs citoyens.

Dans la présente analyse, nous examinons comment d'autres pays que le nôtre ont procédé et nous faisons état des enjeux et défis qu'apporte la mise en œuvre de la portabilité des données. À la lumière de ces éclairages, nous regardons également comment les mises en pratique à l'étranger peuvent guider l'élaboration d'un modèle d'approche proprement canadien.

En résumé, nos principales observations sont les suivantes :

- La portabilité des données pourrait stimuler l'innovation chez les entreprises canadiennes et produire des avantages économiques.
- Les entreprises canadiennes bénéficieraient de définitions claires quant aux types de données et au degré de détail qu'elles devront rendre transférables, définitions établies, dans une certaine mesure, en fonction de l'utilité potentielle future des données pour les personnes concernées.
- Quand les entreprises qui contrôlent les données s'assurent que les utilisateurs sont bien ceux qu'ils prétendent être, elles atténuent des risques lourds à l'égard de la vie privée et de la cybersécurité, étant donné que des cybercriminels peuvent tenter d'exploiter les processus de transfert de données pour accéder à des données de nature sensible qui relèvent de particuliers et d'entreprises. Des normes sectorielles d'authentification pourraient apporter plus de clarté et alléger ce fardeau de l'authentification des utilisateurs.
- La mise en place et la mise à jour des processus de traitement des demandes de portabilité des données constituent l'un des coûts les plus importants pour les entreprises. Ces dépenses pourraient être réduites en fixant des normes claires relatives au format technique des transferts de données.
- Les entreprises ont besoin de clarté au sujet de leurs responsabilités juridiques quant au sort des données qu'elles transfèrent à d'autres. Des moyens devraient être mis en place pour que les organisations réceptrices de données puissent montrer qu'elles disposent de capacités adéquates afin d'assurer la protection et la confidentialité des données (par exemple, codes de conduite et accréditation).
- Pour réduire le fardeau des entreprises canadiennes qui doivent se conformer à de multiples régimes de portabilité des données, la réglementation fédérale devrait être harmonisée aux règles en vigueur ou en préparation dans les provinces et chez les principaux partenaires commerciaux du pays.

En définitive, comme l'ont souligné les participants à un atelier organisé par la Federal Trade Commission (FTC) aux États-Unis (Commission fédérale du commerce), les risques liés à la protection de la vie privée et à la cybersécurité pourraient compromettre les avantages de la portabilité des données, ce qui souligne l'importance d'un juste équilibre entre la réduction de ces risques et la maximisation des objectifs de protection de la vie privée, d'innovation et de concurrence<sup>1</sup>.

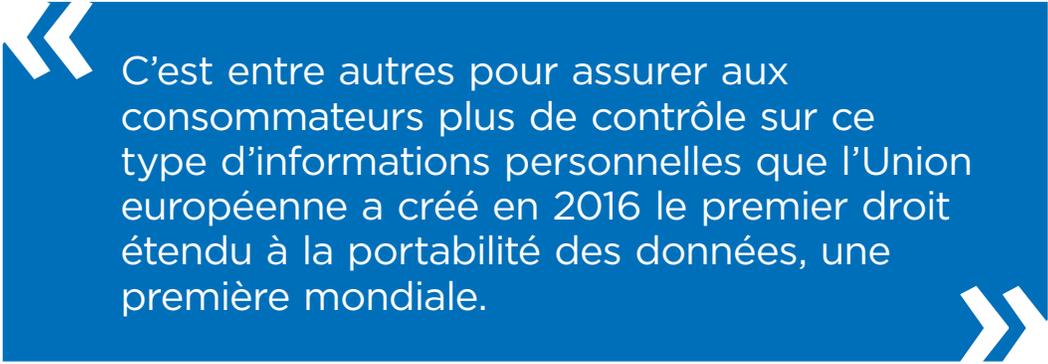
Dans notre étude, vu le contexte en évolution rapide, nous arrivons à la conclusion que le gouvernement fédéral devrait construire son approche de réglementation de la portabilité des données en se servant des enseignements que livrent les expériences d'autres pays et en consultant étroitement les entreprises innovantes et les autres parties prenantes.

1 Gabe Maldoff, Jayne Ponder, Kayvan Farchadi et Claire O'Rourke, « [Five Key Themes from the FTC's Data Portability Workshop](#) », *Inside Privacy*, 30 septembre 2020.

# La portabilité des données : qu'est-ce que c'est, et quelle est son importance?

En février 2018, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a terminé son examen de la LPRPDE et a recommandé un certain nombre de changements importants, en recommandant notamment de conférer aux Canadiens le droit à la portabilité des données.

Selon le rapport final du Comité, « [...] les individus doivent demeurer aussi libres que possible de choisir la façon dont ils disposent de leurs renseignements personnels. Or, cette liberté de choisir ne devrait pas être restreinte à la capacité de consentir à la collecte, l'utilisation et la communication de leurs renseignements personnels ou de retirer ce consentement. Le Comité est d'avis qu'il est aussi important que les individus soient en mesure de transférer leurs renseignements personnels entre prestataires de services de manière à pouvoir les réutiliser<sup>2</sup>. »



C'est entre autres pour assurer aux consommateurs plus de contrôle sur ce type d'informations personnelles que l'Union européenne a créé en 2016 le premier droit étendu à la portabilité des données, une première mondiale.

Il existe de nombreux types de données que les consommateurs peuvent souhaiter transférer d'un fournisseur de services à un autre. Il s'agit non seulement des coordonnées et des informations d'identification de base, mais aussi des historiques et des signets de navigateur Web, des photos avec des marqueurs et des commentaires, des recettes, des listes de lecture,

2 Chambre des Communes, *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, février 2018.

des dossiers bancaires et financiers, des données sur la santé et le bien-être, ainsi que des données provenant des compteurs intelligents et des produits connectés à l'Internet des objets.

C'est entre autres pour assurer aux consommateurs plus de contrôle sur ce type d'informations personnelles que l'Union européenne (UE) a créé en 2016 le premier droit étendu à la portabilité des données, une première mondiale :

*Ce nouveau droit a pour objectif de responsabiliser les personnes concernées et de leur permettre de contrôler davantage les données à caractère personnel les concernant.*

*Dans la mesure où il permet la transmission directe des données à caractère personnel d'un responsable du traitement à un autre, le droit à la portabilité des données constitue également un instrument important qui facilitera la libre circulation des données à caractère personnel dans l'Union et qui stimulera la concurrence entre les responsables du traitement. Il facilitera le passage d'un prestataire de services à un autre et encouragera dès lors la mise au point de nouveaux services dans le contexte de la stratégie pour un marché unique numérique<sup>3</sup>.*

À mesure que les séries de données s'élargissent et que les capacités d'analyse des données englobent des combinaisons d'ensembles de données toujours plus diversifiés, la valeur des données personnelles transférables devrait continuer à augmenter. Pour les consommateurs, les avantages iront au-delà de la commodité et de la facilité à changer de fournisseur, car les entreprises sont de plus en plus aptes à tirer des enseignements des données personnelles pour améliorer leurs produits et services, ainsi que la manière dont elles les fournissent.

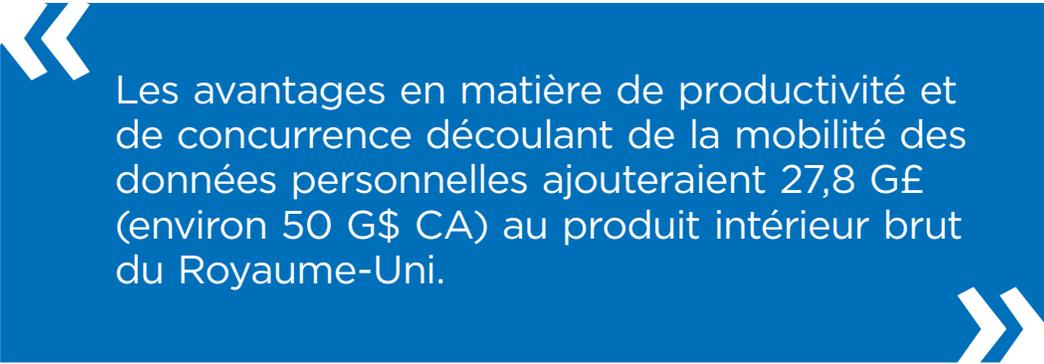
Selon le Data Transfer Project (DTP) (projet de transfert de données)<sup>4</sup>, la portabilité des données ouvre la voie à un large éventail de précieux nouveaux services pour les particuliers. Diverses améliorations sont évoquées :

- des informations étoffées sur la santé et le bien-être, qui regroupent les données des systèmes de santé, des dispositifs électroniques portatifs et d'autres sources;
- une meilleure gestion des finances personnelles grâce à l'accès à des données détaillées sur les opérations et à d'autres données issues de divers comptes et institutions;

<sup>3</sup> Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices relatives au droit à la portabilité des données*, adoptées le 13 décembre 2016; version révisée et adoptée le 5 avril 2017.

<sup>4</sup> Le Data Transfer Project (DTP) (projet de transfert de données) est une initiative collaborative en code source ouvert visant à développer des concepts et des outils pour faciliter les transferts de données en masse contrôlés par les clients entre deux services en ligne. Parmi les membres figurent Google, Facebook, Twitter, Apple et Microsoft.

- un accès élargi aux services publics et privés;
- une surveillance et une transparence accrues à l'égard des données personnelles;
- une sécurisation renforcée des données personnelles, notamment par la sauvegarde ou l'archivage d'informations importantes, ce qui facilite la récupération en cas de détournement de compte<sup>5</sup>.



Les avantages en matière de productivité et de concurrence découlant de la mobilité des données personnelles ajouteraient 27,8 G£ (environ 50 G\$ CA) au produit intérieur brut du Royaume-Uni.

En 2018, un rapport commandé par le gouvernement britannique a conclu que la mobilité des données personnelles « peut être un stimulant essentiel pour faire passer la croissance numérique à la vitesse supérieure<sup>6</sup> ». L'analyse économique dressée dans le rapport indique que les avantages en matière de productivité et de concurrence découlant de la mobilité des données personnelles ajouteraient 27,8 G£ (environ 50 G\$ CA) au produit intérieur brut du Royaume-Uni, et que l'apport de l'innovation numérique engendrée par la mobilité des données personnelles serait probablement encore plus important.

Selon ce même rapport, « la mobilité des données personnelles peut stimuler une croissance nouvelle en créant un environnement où des particuliers responsabilisés feront bon usage en toute sécurité de leurs données personnelles et consentiront à ce que d'autres les utilisent dans le cadre de nouveaux services et technologies axés sur les données. En bref, il s'agit d'offrir des avantages aux particuliers comme aux organisations, pour récolter des gains économiques et sociaux considérables<sup>7</sup>. »

En effet, comme nous le verrons plus loin, on recueille ce genre d'avantages dans certains domaines déjà, grâce, par exemple, à l'initiative du système Open Banking (système bancaire ouvert) lancée au Royaume-Uni.

5 Data Transfer Project, *Data Transfer Project Overview and Fundamentals*, 20 juillet 2018.

6 Ctrl-Shift et Department for Digital, Culture, Media & Sport, *Data Mobility: The personal data portability growth opportunity for the UK economy*, 2018.

7 *Ibid.*

## Portabilité des données ou mobilité des données : quelle est la différence?

Si certains emploient indifféremment les termes de portabilité des données et de mobilité des données, pour d'autres, la mobilité des données prend un sens plus large. Les membres de l'initiative Personal Data Mobility Sandbox du réseau Ctrl-Shift, dont Barclays Bank, la BBC, Centrica, Facebook et d'autres organisations, décrivent la différence comme suit :

*La mobilité des données personnelles va au-delà de la portabilité des données personnelles. En vertu du Règlement général sur la protection des données (RGPD), les particuliers peuvent transférer leurs données personnelles d'un fournisseur à l'autre, mais ce processus tend actuellement à être manuel et ponctuel.*

*Avec la mobilité des données personnelles, les données personnelles circulent de manière sûre et efficiente là où elles peuvent créer une valeur maximale. Ces flux sont contrôlés par le particulier, de sorte que les avantages personnels, sociaux et économiques sont distribués équitablement<sup>8</sup>.*

Nous notons que le projet de loi C 11 du gouvernement fédéral fait référence à la « mobilité des données », alors que dans d'autres pays on parle plutôt de « portabilité des données », comme l'a fait d'ailleurs le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes en 2018.

Dans la présente analyse, nous employons généralement « portabilité des données », sauf dans le contexte du projet de loi C 11 et, le cas échéant, dans les citations directes des sources consultées.



8 Ctrl-Shift, *Data Mobility Infrastructure Sandbox: Report - June 2019*.

# Cadres relatifs à la portabilité des données ailleurs dans le monde

## Approches d'autres pays

On pense généralement qu'à l'instar de plusieurs autres pays, le Canada adoptera une approche de portabilité des données qui s'apparentera au droit qu'instaure l'article 20 du *Règlement général sur la protection des données* (RGPD) de l'UE, entré en vigueur le 25 mai 2018. Selon Daniel J. Michaluk, associé chez Borden Ladner Gervais : « Le Canada n'adoptera pas nécessairement toutes les spécificités du RGPD, mais celui-ci servira manifestement de modèle pour la réforme<sup>9</sup>. »

Le RGPD considère la portabilité des données dans sa plus grande extension et s'applique à un large éventail d'organisations qui traitent des données. Bien que le RGPD ne définisse pas spécifiquement la portabilité des données, un groupe de travail de l'UE précise qu'il s'agit de conférer « [...] aux personnes concernées le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement<sup>10</sup>. » Les dispositions relatives à la portabilité des données basées sur le modèle de l'UE établies par d'autres pays utilisent un langage semblable.

On pense généralement qu'à l'instar de plusieurs autres pays, le Canada adoptera une approche de portabilité des données qui s'apparentera au droit qu'instaure l'article 20 du *Règlement général sur la protection des données* (RGPD) de l'UE.

La *California Consumer Privacy Act* (CCPA), entrée en vigueur le 1<sup>er</sup> janvier 2020, est tout à fait proche du RGPD, mais englobe un plus ample éventail de données privées (par exemple, les enregistrements des interactions de sites

9 Daniel J. Michaluk, Borden Ladner Gervais s.r.l./S.E.N.C.R.L., « [La réforme du droit canadien relatif à la protection de la vie privée est imminente – êtes-vous prêt?](#) », BLG.com, 18 septembre 2020.

10 *Supra*, note 3.

Web ou d'applications<sup>11</sup>). En novembre 2020, des améliorations à la CCPA ont été adoptées dans la *California Privacy Rights Act* (CPRA), qui entrera en vigueur le 1<sup>er</sup> juillet 2023. Comme le RGPD, la CPRA fait référence aux transferts interentreprises d'informations personnelles dans un format structuré, couramment utilisé et lisible par machine (toutefois, la CPRA n'exige le transfert que s'il est réalisable sur le plan technique<sup>12</sup>).

Plusieurs autres États, dont le Washington et le New Jersey, envisagent également d'adopter de nouvelles lois sur la protection de la vie privée. En mars 2020, la Virginie est devenue le deuxième État à adopter une loi sur la protection de la vie privée, qui porte notamment sur la portabilité des données, et l'Utah a un projet de loi semblable à l'étude<sup>13</sup>.

En Australie, en vertu du cadre Consumer Data Right (CDR) (Droit des consommateurs à l'égard de leurs données), entré en vigueur en février 2020, les consommateurs peuvent exiger des détenteurs de données qu'ils transmettent des catégories spécifiques de données sous forme lisible par machine à des prestataires de services accrédités<sup>14</sup>. La mise en œuvre du CDR se fait progressivement, par secteur d'activité, en commençant par le secteur bancaire, qui sera suivi des secteurs de l'énergie et des télécommunications.

L'Inde a choisi une approche différente de la portabilité des données, qui se concentre principalement sur le secteur bancaire. Contrairement au RGPD et à d'autres cadres semblables, la Data Empowerment and Protection Architecture (DEPA) (Architecture d'autonomisation et de protection des données) établie par l'Inde permet le transfert des données des consommateurs entre les institutions financières par un consentement numérique ponctuel pour chaque opération de données plutôt que par un consentement général comme celui du RGPD, pour le transfert et la réutilisation des données<sup>15</sup>. Comme il a été précisé lors de l'atelier sur la portabilité des données tenu par la Federal Trade Commission (FTC) des États-Unis, « en vertu de la DEPA, les utilisateurs peuvent se connecter à des applications autorisées et recueillir leurs données financières – comme l'historique de leurs opérations – qu'ils peuvent ensuite communiquer à une autre entité en vue d'obtenir des prêts et d'autres services financiers<sup>16</sup>. »

11 Maria Korolov, « [California Consumer Privacy Act \(CCPA\): What you need to know to be compliant](#) », CSO, 7 juillet 2020.

12 Wirewheel, « [CPRA vs. CCPA vs. GDPR: How the Difference Impacts Your Data Privacy Options](#) », 2020.

13 Cat Zakrzewski, « [Virginia governor signs nation's second state consumer privacy bill](#) », *The Washington Post*, 2 mars 2021.

14 Linklaters, « [Data Protected – Australia](#) », mars 2020.

15 Competition Policy International, Inc., [Data To Go: The FTC's Workshop on Data Portability](#), *CPI Antitrust Chronicle*, novembre 2020.

16 *Ibid.*

Singapour, Mexique, Argentine, Brésil et Chili, notamment, sont parmi les pays qui ont adopté une législation similaire sur la portabilité des données. Aux États-Unis, la FTC cherche à élaborer un cadre de portabilité des données qui s'appliquerait à l'échelle fédérale, et elle a lancé une série de consultations pour examiner des modèles possibles, comme le RGPD et la CCPA (Californie).

## Prise de mesures par les provinces canadiennes

Au Canada, certaines provinces s'appêtent à revoir leurs lois sur la protection de la vie privée afin de les rendre plus conformes au RGPD<sup>17</sup> :

- Au Québec, le projet de loi n° 64, arrivé à l'étape de l'adoption du principe en octobre 2020, vise à accorder aux consommateurs le droit à la portabilité des données, entre autres changements<sup>18</sup>.
- En Ontario, les consultations sur les propositions visant à améliorer la protection des renseignements personnels, y compris le droit à la portabilité des données, ont pris fin en octobre 2020<sup>19</sup>.
- En décembre 2020, la Colombie-Britannique a mis sur pied un comité spécial chargé d'examiner la *Personal Information Protection Act* en mettant l'accent sur les dispositions du projet de loi C-11. Le comité spécial tiendra également compte des commentaires reçus lors des consultations publiques menées avant les récentes élections<sup>20</sup>.
- En Alberta, le commissaire à l'information et à la protection de la vie privée a demandé, en janvier 2021, une mise à jour de la législation sur la protection de la vie privée, y compris à l'égard de la portabilité des données, en raison « du changement technologique radical provoqué par la pandémie de COVID-19 et d'une tendance visant à modifier la législation semblable dans d'autres pays<sup>21</sup> ».

Bien qu'il y ait du mouvement au Canada et à l'étranger, ces lois sont relativement nouvelles ou ne sont pas encore entrées en vigueur, de sorte que nous disposons de peu d'expériences vécues ou de recherches empiriques à ce jour pour évaluer leur incidence sur les entreprises. Dans les pages suivantes,

17 Au Canada, la *Loi sur la protection de la vie privée des consommateurs* (LPVPC) s'appliquerait, comme la LPRPDE qu'elle remplace, aux sociétés sous réglementation fédérale et aux sociétés fermées dans les provinces et territoires qui n'ont pas leur propre législation sur la protection de la vie privée.

18 Assemblée nationale du Québec, projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, présenté le 12 juin 2020.

19 Gouvernement de l'Ontario, « [Consultation : Renforcer les mesures de protection de la vie privée en Ontario](#) », 13 août 2020 (page Web).

20 Assemblée législative de la Colombie-Britannique, « [Special Committee to Review the Personal Information Protection Act](#) » (page Web).

21 James Swanson, cité dans Anthony Burden, Field s.r.l./S.E.N.C.R.L., « [Alberta's Legislation on Privacy and Protection of Personal Information Needs Review: Commissioner](#) », Mondaq, 7 janvier 2021.

nous explorons quelques-uns des enjeux les plus importants dans d'autres pays dont font état certains articles, études et documents de consultation gouvernementaux librement accessibles.

### **La Loi sur la protection de la vie privée des consommateurs (LPVPC) comparée à d'autres cadres de protection des données personnelles**

Selon leurs lieux d'activité, les entreprises qui contrôlent des données au Canada peuvent devoir se conformer à plusieurs régimes de protection des données, y compris à différentes exigences de portabilité des données. Il peut s'agir de lois fédérales et provinciales du Canada, du RGPD, de la CCPA (Californie) et de régimes fédéraux et étatiques américains en cours d'élaboration.

Lorsque le RGPD est entré en vigueur dans l'UE en 2018, ses normes plus rigoureuses par rapport à la LPRPDE, y compris le nouveau droit à la portabilité des données, ont créé des obstacles pour les entreprises canadiennes qui exercent des activités dans l'espace européen. Depuis, de nombreuses entreprises canadiennes ont harmonisé leurs pratiques de protection de la vie privée au RGPD et, plus récemment, à la LPVPC.

Comme l'a fait remarquer Avery Swartz, conseiller technique auprès de PME, « étant donné que de nombreuses entreprises en ligne exercent leurs activités à l'échelle mondiale, le plus facile, pour elles, c'est d'actualiser leurs conditions d'utilisation afin de satisfaire aux exigences les plus strictes dans tous les pays, au lieu d'avoir des politiques différentes pour différentes régions. Beaucoup choisissent de suivre les règles du RGPD partout. Ces dispositions vont devenir la norme *de facto* pour ce qui est des modalités de confidentialité dans le monde entier, même dans les pays qui ne pratiquent pas de surveillance en la matière<sup>22</sup>. »

En d'autres termes, comme le résume l'avocat James Swanson, les entreprises « se conforment généralement à la norme la plus stricte<sup>23</sup> ». Il ajoute toutefois qu'en affaires, les choses doivent être claires. « Si on a une sorte de mosaïque où l'Alberta a des règles différentes de celles du gouvernement fédéral ou de l'Ontario, les choses se complexifient pour les entreprises. Lorsqu'il y a une certaine uniformité, le commerce en est facilité<sup>24</sup>. »

22 Avery Swartz, « [Europe's GDPR rules mean big changes for businesses in Canada](#) », The Globe and Mail, 17 mai 2018.

23 *Supra*, note 21.

24 *Ibid.*



Plus les lois sur la protection de la vie privée seront harmonisées, moins les entreprises auront de la peine à se conformer à différents régimes de protection des données.

Plus les lois sur la protection de la vie privée seront harmonisées, moins les entreprises auront de la peine à se conformer à différents régimes de protection des données. S'il est important d'élaborer une réglementation fédérale sur la portabilité des données qui sera adaptée au contexte canadien, l'harmonisation de ces règles aux régimes provinciaux et aux autres régimes nationaux devrait contribuer à favoriser l'efficacité et la compétitivité des entreprises canadiennes.

# Mise en œuvre de la portabilité des données : enjeux et défis

Comme le fait valoir la U.S. Chamber of Commerce (Chambre de commerce des États-Unis) dans sa contribution à un atelier organisé par la FTC sur les avantages et les défis potentiels de la portabilité des données, « la mise en œuvre de la portabilité des données est un défi des plus techniques, qui nécessite beaucoup de temps et de ressources<sup>25</sup> ».

Pour les années 2017 à 2019, les organisations qui recueillent et contrôlent des données personnelles ont systématiquement classé la portabilité des données parmi les trois obligations du RGPD les plus difficiles à respecter dans les enquêtes annuelles de l'International Association of Privacy Professionals (IAPP)<sup>26</sup>. Une étude distincte de l'Information Technology and Innovation Foundation (ITIF) a évalué à environ 510 M\$ US le coût de la mise en œuvre à l'échelle fédérale d'une réglementation sur la portabilité des données semblable aux cadres de l'UE et de la Californie<sup>27</sup>.

Il ne fait aucun doute que la conception et la mise à jour de l'infrastructure assurant la portabilité des données et le respect des autres droits des personnes concernées (par exemple, l'accès, la correction et la suppression) occasionneront des coûts aux entreprises. L'ampleur de ces coûts dépendra d'un certain nombre de facteurs, dont beaucoup pourraient être influencés par les règlements d'application. Nous examinons ci-dessous quelques-uns des facteurs les plus importants.

## Champ d'application de la portabilité des données

La mise en place et le maintien d'une infrastructure de gestion des données qui assurera la portabilité des données et le respect des droits des personnes concernées font partie des coûts de conformité les plus importants pour les entreprises<sup>28</sup>. Ces dernières doivent établir des processus leur permettant

25 Chamber of Commerce of the United States of America (U.S. Chamber of Commerce), [Comments to the Federal Trade Commission's Data Portability Workshop](#), 21 août 2020 (lettre).

26 International Association of Privacy Professionals et EY, *IAPP-EY Annual Governance Reports 2017-2019*, accessibles à <https://iapp.org/resources/article/iapp-fti-consulting-privacy-governance-report-2020/>.

27 Alan McQuinn et Daniel Castro, « [The Costs of an Unnecessarily Stringent Federal Data Privacy Law](#) », Innovation Technology & Innovation Foundation, août 2019.

28 *Ibid.*

de stocker, de repérer et de mettre à jour les informations personnelles de leurs clients, et de les transférer dans des formats appropriés à d'autres organisations, à la demande.

Comme l'observe la U.S. Chamber of Commerce, « le processus de révision et de mise en œuvre de nouvelles mesures techniques et de protocoles de gestion des données devient plus complexe et problématique à mesure que l'ensemble des données devant répondre aux exigences de portabilité augmente, tant sur le plan de l'ampleur que sur le plan des détails<sup>29</sup>. »

En général, les régimes actuels de portabilité des données s'appliquent aux informations fournies directement par les utilisateurs, telles que les coordonnées et les préférences, ainsi qu'aux données observées, telles que les historiques de navigation sur Internet. Sont habituellement exclues les données qu'une organisation crée par déduction à l'aide d'algorithmes exclusifs, par exemple pour prédire le comportement d'un utilisateur.

Certains ont recommandé de limiter plus encore l'envergure des données soumises à la portabilité afin de réduire les coûts du traitement des demandes et d'apporter davantage de clarté aux entreprises sur la portée de cette obligation.

Dans un livre blanc publié en 2019, Facebook se demande s'il existe des cas où le fardeau opérationnel pour les entités – en particulier les entreprises en démarrage et les PME – l'emporterait sur l'intérêt du consommateur à exporter ses données. « Ainsi, les données d'utilisation d'un service pourraient inclure la liste de chaque page ou élément de contenu ayant été consulté au cours d'une période donnée, de chaque lien cliqué, de chaque notification reçue [...] Assurer la portabilité de ces données archivées pourrait s'avérer difficile, sans que les avantages pour l'utilisateur soient manifestes<sup>30</sup> [...]. »



Le fait de disposer d'un ensemble bien défini de catégories de données réduira les coûts de conformité et fournira aux particuliers et aux organisations un cadre clair relatif aux données à transférer.

29 *Supra*, note 25.

30 Facebook, *Charting a Way Forward: Data Portability and Privacy*, 2019.

Singapour a traité cette question en appliquant son régime de portabilité des données à des « ensembles de données sur liste blanche », établis en fonction des différents secteurs d'activité par la Personal Data Protection Commission (PDPC) (Commission sur la protection des données personnelles), par les parties prenantes de l'industrie et par d'autres autorités de réglementation concernées. À titre d'exemple, les données sur liste blanche concernant l'historique des dépenses des consommateurs ne comprennent que des données spécifiques sur les achats et les paiements, tandis que les données sur liste blanche concernant l'historique de la consommation des services publics comportent des données spécifiques, telles que les données cellulaires et la consommation d'électricité.

Selon la PDPC, « le fait de disposer d'un ensemble bien défini de catégories de données réduira les coûts de conformité et fournira aux particuliers et aux organisations un cadre clair relatif aux données à transférer en vertu du droit à la portabilité des données<sup>31</sup>. »

Les entreprises canadiennes bénéficieraient de directives claires quant aux types et au degré de détail des données qu'elles doivent rendre portables, en se basant dans une certaine mesure sur l'utilité potentielle future des données pour les personnes qui en font la demande.

## Processus d'authentification du client

Les problèmes d'authentification sont constamment cités comme l'une des principales préoccupations des entreprises devant effectuer le transfert de données, y compris dans l'enquête 2020 de l'IAPP auprès des organisations contrôlant des données<sup>32</sup>. Pour préserver la confidentialité des données et prévenir d'éventuelles atteintes à la cybersécurité, il est essentiel que les entreprises vérifient que la personne qui demande un transfert de données est bien celle qu'elle prétend être. C'est d'autant plus impératif que des cybercriminels peuvent tenter d'utiliser le processus de transfert de données pour attaquer les systèmes informatiques d'une organisation et accéder ainsi à des informations de nature sensible, qu'elles relèvent d'une personne ou d'une entreprise.

Un participant à l'atelier de la FTC sur la portabilité des données<sup>33</sup> tenu en 2020 a observé que l'authentification des clients constituait un obstacle important à l'utilisation du système Open Banking du Royaume-Uni par les particuliers, surtout lorsqu'ils devaient passer par de multiples étapes pour

31 Personal Data Protection Commission (Singapour), *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions*, 20 janvier 2020.

32 International Association of Privacy Professionals et FTI Consulting, *IAPP-FTI Consulting Privacy Governance Report 2020*, décembre 2020.

33 *Supra*, note 15.

autoriser leur banque à transférer leurs données. Des difficultés semblables ont été constatées dans le secteur de la santé au Royaume-Uni, tant pour les patients que pour les organisations qui contrôlent des données.

Combinaisons de bases de données de référence, appariement de données, identification biométrique et authentification multifactorielle sont au nombre des méthodes mises à l'essai actuellement par le secteur privé. Un participant à l'atelier a toutefois fait remarquer que, dans le secteur financier, ces méthodes alourdiraient les coûts, tant pour les institutions financières que pour les clients, ce qui pourrait limiter l'accès aux données pour ces derniers.

De nombreuses institutions financières ont adopté voilà des années des processus visant à respecter les exigences de connaissance du client pour lutter contre la criminalité financière et le blanchiment d'argent. Si l'authentification reste un défi coûteux pour les grandes institutions financières disposant de cadres établis et de ressources importantes pour respecter le principe de la connaissance du client, du point de vue des PME qui doivent élaborer des processus à partir de zéro, le coût et les difficultés d'un tel projet seraient naturellement plus considérables encore. Comme nous l'avons déjà souligné dans un mémoire présenté au gouvernement fédéral, « [...] certaines entités de petite taille, comme des PME, des organismes non gouvernementaux et des œuvres de bienfaisance, pourraient bien ne pas posséder les ressources nécessaires (technologie, littératie numérique, compétences) pour transférer des renseignements personnels à une autre organisation de façon sûre et efficace<sup>34</sup>. » Cela risque bien sûr de nuire à la capacité des petites organisations à mettre en place des processus d'authentification et des systèmes de cybersécurité robustes. De ce fait, elles seront plus vulnérables, les cybercriminels cherchant à cibler et à exploiter leurs failles numériques.

Les demandes de transfert de données effectuées par une personne pour le compte d'une autre suscitent également des inquiétudes en matière de sécurité. Plusieurs répondants qui ont participé à la consultation de Singapour sur la confidentialité des données se sont interrogés sur la manière dont les demandes de transfert de données seraient traitées, par exemple pour les titulaires de comptes conjoints, les titulaires de cartes de crédit supplémentaires, les assurés et les exécuteurs testamentaires<sup>35</sup>.

Dans la consultation de la FTC, il a été proposé que, dans le cadre d'un nouveau régime américain de portabilité des données, le gouvernement fédéral établisse des normes pour donner aux banques des directives claires

34 CPA Canada, *Mémoire soumis en réponse à : Renforcer la protection de la vie privée dans l'ère numérique*, janvier 2020.

35 *Supra*, note 31.

quant aux procédures d'authentification appropriées. Des normes sectorielles semblables pourraient apporter davantage de précisions et alléger le fardeau de l'authentification des utilisateurs dans d'autres secteurs d'activité<sup>36</sup>.

## Allègement du fardeau du traitement administratif pour les entreprises

Dans l'estimation faite par l'ITIF des coûts pour les entreprises américaines d'un régime fédéral de portabilité des données, la plus grande part des coûts prévus, soit 340 M\$ US sur un total de 510 M\$ US, sont le fait du traitement des demandes des personnes concernées. L'ITIF note que ces demandes ne seront pas seulement effectuées en ligne, mais aussi par téléphone, par courrier ou en personne, et que l'intervention humaine peut faire fortement augmenter les coûts<sup>37</sup>.

« Dans l'estimation faite par l'ITIF des coûts pour les entreprises américaines d'un régime fédéral de portabilité des données, la plus grande part des coûts prévus, soit 340 M\$ US sur un total de 510 M\$ US, sont le fait du traitement des demandes des personnes concernées. »

Les organisations visées doivent veiller à la mise en place et au maintien de l'infrastructure nécessaire pour assurer la portabilité des données et traiter les autres demandes des personnes concernées. Dans le contexte du RGPD, l'expérience a montré que ces processus peuvent accroître de beaucoup la charge de travail pour bien des entreprises. Dans l'enquête 2020 de l'IAPP auprès des organisations soumises au RGPD qui contrôlent des données, 62 % des répondants ont déclaré avoir des équipes affectées au traitement des demandes des personnes concernées, ce qui représente une augmentation notable par rapport à l'année précédente (52 %)<sup>38</sup>.

<sup>36</sup> *Supra*, note 15.

<sup>37</sup> *Supra*, note 27.

<sup>38</sup> International Association of Privacy Professionals et FTI Consulting, *IAPP-FTI Consulting Privacy Governance Report 2020*, décembre 2020.

Malgré la présence d'équipes affectées à la tâche, bon nombre de ces organisations ont pris beaucoup de temps à traiter les demandes des personnes concernées. Si environ 30 % d'entre elles ont répondu dans les deux jours, un peu plus de la moitié ont mis entre deux jours et deux semaines, et 12 % ont mis un mois ou plus. Environ la moitié des répondants font appel à l'automatisation, dans une certaine mesure, pour traiter les demandes; chez les autres, les processus sont entièrement manuels.

Sur les demandes reçues en 2020 par ces entreprises, 15 % portaient sur le transfert de données. Une étude distincte de 2019 sur les retentissements du RGPD dans la pratique montre que les demandes de portabilité des données présentent des défis particuliers<sup>39</sup>. Pour cette étude, les chercheurs ont fait 230 demandes réelles de transfert de données et ont examiné comment les entreprises y ont répondu. Environ 75 % des demandes seulement ont été menées à bien. Même parmi ces demandes, de nombreux formats de fichiers ne répondaient pas aux exigences du RGPD. Les chercheurs ont également constaté qu'il régnait une certaine confusion au sein de ces entreprises concernant les droits des consommateurs en matière de données, de manière plus générale.

Ces résultats concordent avec les propres conclusions de la Commission européenne, en 2020, dans son examen de l'application du RGPD<sup>40</sup>. La Commission a constaté que de nombreuses organisations contrôlant des données avaient du mal à respecter l'obligation de fournir des données dans « un format structuré, couramment utilisé, lisible par machine » en raison de l'absence de normes sur ce point, vu que le format varie considérablement selon les secteurs d'activité. La Commission a également constaté que seules les organisations de certains secteurs – tels que les services bancaires, les télécommunications et les services publics – avaient mis en place les interfaces nécessaires pour répondre aux demandes de transfert de données dans un format approprié.

En raison des considérations énoncées par la Commission, la stratégie européenne pour les données, adoptée en février 2020, rend obligatoire l'élaboration d'interfaces techniques et de formats lisibles par machine permettant la portabilité des données. Cependant, même si les entreprises ont commencé à fournir leurs données dans des formats structurés, couramment

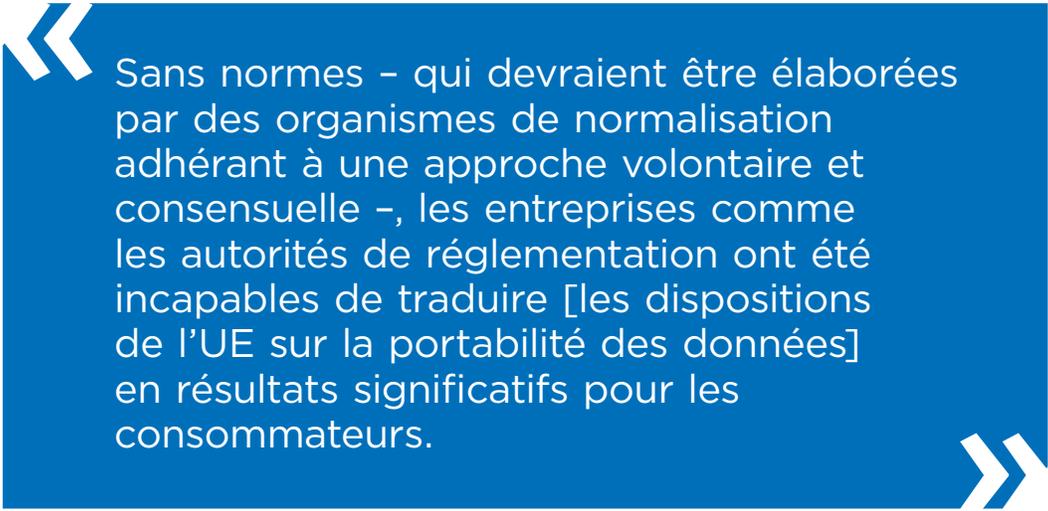
39 Janis Wong et Tristan Henderson, « [The right to data portability in practice: exploring the implications of the technologically neutral GDPR](#) », School of Computer Science, University of St Andrews, 22 mai 2019.

40 Commission européenne, [La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données](#), 24 juin 2020.

utilisés et lisibles par machine pour se conformer au RGPD ou à une législation du même ordre, il a été observé que, dans la plupart des cas, ces formats ne sont pas compatibles entre eux<sup>41</sup>.

Les chercheurs de l'étude pratique de 2019 ont de même conclu que des travaux futurs étaient nécessaires pour aider les responsables du traitement des données à se conformer au droit à la portabilité des données : « Nous recommandons que les différentes parties prenantes travaillent ensemble pour décider de la méthode la plus appropriée pour soutenir le [droit à la portabilité des données], que ce soit l'élaboration de lignes directrices, de normes ou de codes de conduite. Des recherches empiriques plus poussées [...] permettraient d'avoir une vision plus globale du [droit] dans la pratique<sup>42</sup>. »

Dans sa présentation à la FTC, la U.S. Chamber of Commerce demande également la création de normes techniques appropriées dans le cadre d'un éventuel régime fédéral américain de portabilité des données. « Sans normes – qui devraient être élaborées par des organismes de normalisation adhérant à une approche volontaire et consensuelle –, les entreprises comme les autorités de réglementation ont été incapables de traduire [les dispositions de l'UE sur la portabilité des données] en résultats significatifs pour les consommateurs<sup>43</sup>. »



Sans normes – qui devraient être élaborées par des organismes de normalisation adhérant à une approche volontaire et consensuelle –, les entreprises comme les autorités de réglementation ont été incapables de traduire [les dispositions de l'UE sur la portabilité des données] en résultats significatifs pour les consommateurs.

Compte tenu de l'expérience de l'UE, certains ont fait valoir que des problèmes semblables pourraient survenir au Canada si les questions relatives à l'interopérabilité des données n'étaient pas clarifiées. Selon l'ancienne commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, et Julie Uzan-Naulin, avocate chez Fasken, « l'exercice de ce droit à la portabilité

41 Data Transfer Project, [Why do we need the DTP](#) (page Web).

42 *Supra*, note 39.

43 *Supra*, note 25.

s'est avéré déjà assez difficile dans l'Union européenne. Il risque de l'être encore plus au Québec et au Canada en l'absence de directives techniques détaillées des autorités de protection des données, ou encore de normes ou codes technologiques partagés par les entreprises<sup>44</sup>. »

Un rapport commandé par le gouvernement britannique a exprimé un point de vue semblable en 2018 : « L'établissement de normes, de technologies et de services tout à la fois solides et communs est essentiel à la création d'un marché en santé, centré sur la mobilité des données personnelles. Tant que ces normes, technologies et services ne sont pas au point, les risques et les coûts associés à la mobilité des données pour toutes les parties prenantes augmentent considérablement, et le rythme de développement du marché et d'accès aux occasions ralentit beaucoup<sup>45</sup> ».

## Interfaces de protocole d'application et plateformes interopérables

Le système Open Banking du Royaume-Uni (système bancaire ouvert), qui s'appuie sur des normes communes pour les interfaces de protocole d'application (API), les formats de données et la sécurité, met l'accent sur l'importance des API sécurisées et des technologies en code source ouvert dans la mise en œuvre de la portabilité des données. Ce projet a été lancé à la suite d'une enquête de la Competition and Markets Authority (CMA) (Autorité des marchés et de la concurrence) qui a révélé que les plus anciennes et les plus grandes banques du Royaume-Uni profitaient du fait que les consommateurs changent rarement d'institution financière, même si les frais sont élevés.

Comme le précise un mémoire présenté à la FTC, « la CMA a demandé aux neuf principales banques du Royaume-Uni de développer des API [...] qui permettraient aux clients de transmettre en toute sécurité leurs données financières à des tiers réglementés, afin qu'un éventail élargi de fournisseurs de services financiers puissent se faire concurrence. Deux ans après la mise en œuvre, on compte plus d'un million d'utilisateurs actifs du système Open Banking et plus de 700 fournisseurs de services bancaires ouverts, et aucun incident de sécurité notable ne s'est produit<sup>46</sup>. »

44 Julie Uzan-Naulin et Jennifer Stoddart, Fasken s.r.l./S.E.N.C.R.L., « [Le droit à la portabilité, une réelle portabilité ou une simple modernisation du droit d'accès?](#) », 14 septembre 2020.

45 *Supra*, note 6.

46 *Supra*, note 15.

Le système Open Banking existe depuis trois ans, et le nombre d'utilisateurs approche des trois millions. Selon un responsable de l'autorité de mise en œuvre du système, « [...] les consommateurs et les PME voient déjà les avantages de l'écosystème et des fonctionnalités que nous avons mis en place. Ce travail sert de modèle naturel pour montrer comment le principe de "l'ouverture" peut être étendu à tout, de la finance ouverte aux télécommunications ouvertes, donnant ainsi aux clients un plus grand contrôle et de plus grands avantages<sup>47</sup>. »

L'utilisation d'API et de plateformes interopérables accroît l'utilité de la portabilité des données, car elles permettent le transfert de données utilisables en temps réel, plutôt que d'informations statiques et momentanées que les entreprises réceptrices pourraient ne pas être en mesure de réutiliser. En l'absence d'API, les transferts de données sont parfois effectués par capture de données d'écran, ce qui oblige les utilisateurs à communiquer leurs identifiants de connexion avec des tiers pour leur permettre d'accéder à leurs données et de les collecter sur différentes plateformes (principalement des plateformes bancaires en ligne). Au Canada, comme l'ont fait ressortir les témoignages entendus par le Comité sénatorial permanent des banques et du commerce lors de son étude de 2019 sur le système bancaire ouvert, la capture de données d'écran augmente les risques d'usurpation d'identité et de fraude ainsi que les risques de cybersécurité<sup>48</sup>. Teresa Scassa, professeure à l'Université d'Ottawa, l'a fait observer : « Un cadre réglementé pour la mobilité des données est considéré comme étant beaucoup plus sûr [que la capture de données d'écran], car des protections peuvent être intégrées au système, et on peut valider l'identité des participants pour s'assurer qu'ils respectent les normes de sécurité et de confidentialité<sup>49</sup>. »

L'utilisation d'API et de plateformes interopérables accroît l'utilité de la portabilité des données, car elles permettent le transfert de données utilisables en temps réel.

47 Open Banking, « [Three years since PSD2 marked the start of Open Banking, the UK has built a world-leading ecosystem](#) », 13 janvier 2021 (page Web).

48 Rapport du Comité sénatorial permanent des banques et du commerce, *Un système bancaire ouvert, qu'est-ce que cela signifie?*, juin 2019.

49 Teresa Scassa, « [Data Mobility \(Portability\) in Canada's Bill C-11](#) », 12 janvier 2021 (page Web).

Des projets de collaboration tels que le Data Transfer Project (DTP) (Projet de transfert de données) sont en cours pour développer des API communes, des plateformes interopérables et d'autres infrastructures nécessaires. L'objectif du Projet est de développer une plateforme de portabilité des données de service à service, en code source ouvert, qui rend le transfert de données réalisable sur le plan technique, à l'échelle de toutes les organisations, en théorie. Au Royaume-Uni, l'initiative Data Mobility Sandbox du réseau Ctrl-Shift réunit des entreprises, des administrations publiques, des associations de défense de consommateurs et des particuliers pour concevoir et tester l'infrastructure et les outils nécessaires pour faciliter la portabilité des données et accorder plus de contrôle aux consommateurs.

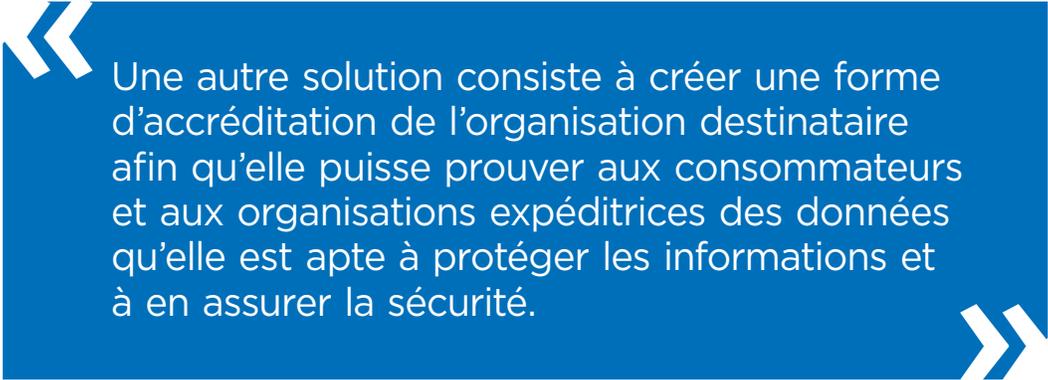
### Attestation de la compétence des destinataires des données transférées

Aux difficultés qui se présentent pour s'assurer que les données sont fournies dans des formats utilisables par les destinataires s'ajoutent des questions sur la part de responsabilité des organisations qui transfèrent des données personnelles. Par exemple, les participants à un atelier de la FTC se sont demandé quels seraient les risques et les responsabilités que les expéditeurs de données auraient à assumer s'ils devaient transférer des données à un fournisseur de services dont les protections en matière de confidentialité ou de cybersécurité sont inadéquates. Des questions et préoccupations ont également été soulevées quant à la responsabilité des expéditeurs de données en cas de transferts ultérieurs ou d'autres utilisations en aval des données transférées<sup>50</sup>.

Certains participants aux consultations de Singapour sur la portabilité des données ont souligné la nécessité d'une définition claire des limites de responsabilité pour les organisations qui transfèrent les données dans l'exécution de leurs obligations. Ces participants ont aussi demandé des précisions sur les responsabilités en cas de fuite des données résultant du transfert des données, ainsi que sur les responsabilités à l'égard de l'exactitude des données transférées à une autre organisation. La PDPC de Singapour a déclaré que les destinataires des données auraient les mêmes obligations que pour toutes les autres données à caractère personnel en leur possession, à savoir les protéger, garantir leur exactitude et ne les utiliser qu'aux fins indiquées.

<sup>50</sup> *Supra*, note 15.

La PDPC établit également des codes de conduite sectoriels contraignants pour la protection des consommateurs, la certification à l'égard des contreparties, l'interopérabilité et la sécurité des données, qui obligent les entités à avoir des protections en place avant de pouvoir recevoir des données demandées par les utilisateurs. Rappelons que ces codes ne s'appliquent qu'aux « ensembles de données sur liste blanche » définis par la PDPC en collaboration avec les parties prenantes et les autorités de réglementation sectorielles.



Une autre solution consiste à créer une forme d'accréditation de l'organisation destinataire afin qu'elle puisse prouver aux consommateurs et aux organisations expéditrices des données qu'elle est apte à protéger les informations et à en assurer la sécurité.

Une autre solution consiste à créer une forme d'accréditation de l'organisation destinataire afin qu'elle puisse prouver aux consommateurs et aux organisations expéditrices des données qu'elle est apte à protéger les informations et à en assurer la sécurité. L'Australie a récemment proposé des modifications à son CDR afin d'offrir aux fournisseurs de services des cheminements pour devenir des « destinataires de données accrédités », selon différents niveaux d'accréditation, de manière à faciliter la tâche des jeunes entreprises et des petits fournisseurs. D'après ces propositions, la Australian Competition & Consumer Commission (Commission australienne de la concurrence et de la consommation) sera chargée d'accréditer les destinataires potentiels des données, d'établir et de tenir à jour un registre des personnes accréditées, et de contrôler et de faire respecter la conformité.

Au-delà des dispositions spéciales prévues par l'Australie pour soutenir les entreprises en démarrage et les PME, il faut souligner que nombre d'entre elles ne disposent pas des ressources financières, des compétences, du temps ou des savoirs nécessaires pour demander une accréditation. Cette situation, qui crée un fardeau à leur charge et décourage d'entrée de jeu les nouveaux arrivants, de moindre envergure, risque de freiner la concurrence que la portabilité des données était censée faciliter.

# Conclusion

La présente étude a voulu mettre en évidence certains coûts et risques considérables qu'un nouveau régime de portabilité des données pourrait représenter pour les entreprises canadiennes. Toutefois, la portabilité des données, si elle est étayée par un ensemble de règlements bien conçus, devrait stimuler l'innovation parmi ces entreprises et se traduire par des avantages économiques.

Comme l'indique le livre blanc de Facebook :

*Pour créer des outils de portabilité que les consommateurs, mis en confiance, seront à même d'utiliser efficacement, il nous incombe d'élaborer des règles claires sur les types de données qui doivent être portables et sur les responsabilités des entités chargées de les protéger lorsqu'elles cheminent entre différents fournisseurs.*

*Sans une infrastructure propice, la portabilité des données soulève de nouveaux risques pour les consommateurs, les organisations et les gouvernements. Ce n'est qu'en travaillant ensemble que ces parties prenantes pourront créer un marché qui permettra de tirer avantage du virage à la portabilité des données<sup>51</sup>.*

Le rapport commandé par le gouvernement britannique a souligné qu'il fallait veiller à ce que la réglementation sur les données soit actualisée et structurée de manière à alimenter la croissance. « Étant donné l'évolution rapide que connaît le marché des données personnelles, en émergence, une approche traditionnelle de la réglementation ne fera que créer des obstacles et limiter le potentiel du marché<sup>52</sup>. »

Le rapport recommande de mettre au point une structure réglementaire par l'intermédiaire d'une consultation et d'une collaboration étroites entre le gouvernement, les innovateurs et les autorités de réglementation, suivies d'un examen régulier des dispositions pour soutenir les progrès de la portabilité des données.

51 *Supra*, note 30.

52 *Supra*, note 6.

Dans l'élaboration de son modèle de réglementation de la portabilité des données au Canada, nous sommes d'avis que le gouvernement fédéral aurait intérêt à tenir compte des initiatives menées dans les autres pays dont il est question dans la présente étude. Vu la numérisation rapide et continue de notre économie, le gouvernement sera appelé à travailler de concert avec des organisations et des regroupements sectoriels pour que les consommateurs puissent profiter en toute sécurité des avantages que la portabilité des données peut leur procurer; il s'agira aussi d'alléger le fardeau des entreprises du Canada et de les amener à exploiter de nouvelles occasions fructueuses.



**CPA**

COMPTABLES  
PROFESSIONNELS  
AGRÉÉS  
CANADA

277, RUE WELLINGTON OUEST  
TORONTO (ONTARIO) CANADA M5V 3H2  
TÉL. : 416 977.3222 TÉLÉC. : 416 977.8585

[CPACANADA.CA](http://CPACANADA.CA)

