LA PROTECTION DE LA VIE PRIVÉE DANS UN SYSTÈME BANCAIRE OUVERT CANADIEN

Publié le 18 octobre, 2021

Catégories: Perspectives, Publications

En août, le Comité consultatif sur un système bancaire ouvert du Canada (le « **Comité** ») a publié son rapport final (le « **Rapport final** »), dans lequel il formule des recommandations pour la mise en place d'un système bancaire ouvert au pays. Aux dernières élections, les libéraux ont promis que s'ils étaient réélus, ils lanceraient d'ici le début de 2023 un « modèle canadien » de système bancaire ouvert. Le gouvernement étant demeuré libéral, le projet devrait poursuivre sa route.

Le présent bulletin est consacré aux questions de la protection de la vie privée et de la sécurité des données dans un tel système et aux changements que les institutions financières et les entreprises de technologie financière (ci-après les « fintechs ») devraient apporter en conséquence. Consultez aussi notre bulletin d'août 2021, qui présente un résumé des recommandations formulées dans le Rapport final, et ceux de février et de juillet 2019, qui traitent du système bancaire ouvert de façon plus générale.

Qu'est-ce qu'un système bancaire ouvert?

Un système bancaire ouvert est un cadre réglementaire qui offre aux particuliers et aux entreprises un moyen sécurisé de transmettre des données bancaires et des données sur des opérations à des tiers autorisés. Un accès sécurisé à l'information permettrait aux fintechs de concevoir une nouvelle gamme d'applications et de produits qui profiteront aux particuliers et aux entreprises. Suivi budgétaire, aide fiscale, nouvelles façons d'évaluer la capacité financière et gestion de la dépendance sont parmi les possibilités.

Pour se procurer les données financières des consommateurs, certaines fintechs procèdent actuellement par « grattage d'écran », une technique rudimentaire qui consiste à copier les renseignements qui se trouvent dans un compte financier. Elle présente un risque important pour la vie privée des consommateurs, qui doivent souvent communiquer leur identifiant et leur mot de passe. Ils risquent aussi de n'avoir aucun recours en cas de consultation non autorisée ou d'utilisation malveillante de leurs données[1]. Un système bancaire ouvert leur offrirait des mesures de sécurité améliorées en plus d'accroître la concurrence dans le secteur financier.

Système bancaire ouvert et vie privée

Comme un système bancaire ouvert repose sur la libre circulation des données, la protection de la vie privée devient essentielle. Dans le cadre de l'Examen des mérites d'un système bancaire ouvert réalisé par le Comité en février 2019, il a été souligné que « [l]a confiance nécessaire pour permettre à l'économie numérique de prospérer et l'acceptation sociale dont les organisations auront besoin de la part des Canadiens pour innover avec leurs données personnelles dépendent de la mise en place d'un cadre juridique approprié qui met à l'avant-plan des questions clés en matière de protection de la vie privée ». Les mémoires de tous les intervenants, lus par le Comité en janvier 2020, citent la protection de la vie privée comme risque important[2]. Celui du Commissariat à la protection de la vie privée du Canada (le « **CPVP** ») fait état de réformes qu'il estime nécessaires en la matière pour qu'un tel système fonctionne[3].

Nombre de ces réformes sont déjà en branle. Avant de déclencher les élections, le gouvernement avait présenté une refonte de la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** ») dans le cadre du projet de loi C-11, qui aurait servi à édicter la *Loi sur la protection de la vie privée des consommateurs* (« **LPVPC** ») (les changements proposés sont résumés dans un précédent bulletin). Le projet de loi C-11 est mort au feuilleton en raison de la dissolution du Parlement. Cela dit, comme les libéraux ont été réélus, on peut supposer qu'un nouveau projet de loi sera présenté. Il y a aussi des pressions internationales pour la réforme des mesures de protection de la vie privée, étant donné que l'UE doit évaluer le caractère adéquat du régime canadien aux termes du Règlement général sur la protection des données (« **RGPD** »). Le maintien du caractère adéquat est essentiel, puisqu'il permet le transfert de données traitées conformément au RGPD de l'UE au Canada sans mesures de protection ou autorisations supplémentaires.

Au Québec, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (le « **projet de loi n° 64** ») a reçu la sanction royale le 22 septembre 2021. Elle modifie la *Loi sur la protection des renseignements personnels dans le secteur privé* (la « **loi québécoise visant le secteur privé** »), notamment en y ajoutant un droit à la portabilité des données, en augmentant les amendes en cas d'infraction et en accentuant les obligations en matière d'avis en cas d'atteinte, de consentement et de protection des données.

À quels autres changements peut-on s'attendre d'ici l'instauration d'un système bancaire ouvert au Canada? Que devront faire les éventuels participants pour s'y ajuster?

Portabilité des données

Dans son rapport de juin 2019 sur le système bancaire ouvert, le Comité sénatorial permanent des banques et du commerce recommande de moderniser la LPRPDE pour la mettre au diapason des normes internationales. Selon lui, les changements devront « inclure [...] le droit à la portabilité des données ».

Dans le contexte d'un système bancaire ouvert, il s'agit du droit d'un consommateur de demander que ses données financières personnelles soient communiquées à une autre organisation. Malgré son apparente simplicité, la portabilité peut être complexe pour l'organisation qui transmet les données (généralement l'institution financière).

Premièrement, les renseignements personnels du consommateur sont souvent groupés avec des renseignements appartenant à l'organisation. Par exemple, les institutions financières créent parfois des « données dérivées » en appliquant leurs algorithmes et leurs analyses aux renseignements des consommateurs[4]. On conclut dans le Rapport final qu'elles devraient pouvoir exclure ce genre de données du système ouvert. Toutefois, si ces données sont normalement à la disposition du consommateur, l'institution devrait être tenue de justifier l'exclusion[5].

Deuxièmement, et dans la même veine, il existe une multitude de formats pour le stockage et le traitement des données, alors qu'une portabilité efficace suppose le transfert dans une forme technologique utilisable. La différence entre une suite de données désorganisées et une feuille de calcul bien montée se fait sentir dans l'utilité des renseignements pour un tiers qui veut créer une application. Les institutions financières peuvent consulter le projet de loi n° 64 pour voir comment le concept de portabilité pourrait s'articuler en pratique. À son entrée en vigueur, le projet de loi n° 64 modifiera la loi québécoise visant le secteur privé en accordant aux consommateurs le droit d'obtenir leurs renseignements personnels informatisés dans un « format technologique structuré et couramment utilisé », sauf en cas de difficultés pratiques sérieuses[6].

L'arrivée d'un droit à la portabilité des données obligera peut-être les institutions financières à revoir leurs systèmes de traitement des données pour s'assurer qu'elles peuvent être communiquées dans un format couramment utilisé et isoler celles qui ne sont pas nécessaires ou qui lui appartiennent exclusivement. Selon le système de traitement des données déjà en place au sein de l'organisation qui transmet les données, la mise en œuvre de la portabilité des données peut prendre un certain temps. Les réalités exposées ci-dessus expliquent sans doute que la modification à la loi québécoise visant le secteur privé qui a trait au format des données n'entrera en vigueur que le 22 septembre 2024, un an après la majorité des dispositions.

Sécurité des données

D'un point de vue technique, un système bancaire ouvert suppose que les institutions financières donnent gratuitement accès à leur interface de programmation d'applications (« **API** ») à des tiers autorisés et accrédités. Forcément, une connectivité accrue amène des risques accrus de fraude, de crime financier et de fuite de données.

Par ailleurs, la LPRPDE oblige les organisations à mettre en place des mesures de sécurité qui correspondent

au degré de sensibilité des renseignements[7], et les renseignements financiers sont considérés comme étant « extrêmement sensibles » par le CPVP et la Cour suprême du Canada[8]. Par conséquent, les participants d'un système bancaire ouvert doivent s'attendre à être visés par des règles strictes.

Les mesures minimales suggérées dans le Rapport final sont l'authentification, l'autorisation, le chiffrement et la journalisation. Pour ce qui est des risques opérationnels, le Rapport final suggère une amélioration des infrastructures de sécurité de TI, un suivi des interventions en cas d'incident et des tests d'intrusion.

Les institutions financières bien établies sont déjà habituées à la plupart de ces mesures de protection, mais les plus petites entreprises voulant participer au système pourraient trouver l'obligation plutôt lourde. Les entreprises qui voudront profiter du système bancaire ouvert pour concevoir de nouvelles solutions de technologie financière devraient penser à ces mesures dès le premier jour.

Responsabilité

Une question importante se pose lors de la conception d'un système bancaire ouvert : qui assumera la responsabilité de la consultation ou de la communication non autorisée de données? Dans son Rapport final, le Comité suggère que la responsabilité suive les données et incombe à la partie fautive. Il recommande que la priorité soit la protection des consommateurs et l'accès à un recours. Dans cette optique, l'institution financière ou le fournisseur de services tiers (selon le cas) devrait être tenu de rembourser sans délai au consommateur la perte financière qu'il a subie, puis de collaborer avec la partie concernée (ou, au besoin, s'engager dans un processus de règlement extrajudiciaire) pour obtenir une indemnisation[9].

Le Comité recommande en outre que le régime de responsabilité s'harmonise avec les lois et les directives provinciales. Par conséquent, ceux qui souhaitent participer au futur système bancaire ouvert ont avantage à comprendre comment les lois sur la protection de la vie privée au Canada attribuent la responsabilité en cas de violation par les fournisseurs de services d'une organisation.

Consentement

Dans son Rapport final, le Comité suggère de mettre en place des règles précises sur l'obtention du consentement des consommateurs. Parmi celles-ci :

- l'emploi d'un langage clair, simple et non trompeur;
- la présentation de renseignements de base, comme les données nécessaires, la raison de cette nécessité, la durée de l'utilisation et les risques potentiels de la communication de ces données;
- des processus normalisés de consentement;
- un système robuste de gestion du consentement (comme un tableau de bord).

Ces idées correspondent aux lois et directives fédérales actuelles en matière de vie privée. Lorsqu'une organisation recueille des renseignements sensibles, la LPRPDE exige généralement l'obtention d'un consentement exprès[10], et les Lignes directrices pour l'obtention d'un consentement valable du CPVP exigent déjà que les points mentionnés ci-dessus soient portés à la connaissance du consommateur d'une façon claire et facile à comprendre. De plus, les lois applicables obligent déjà les organisations qui traitent des renseignements personnels sensibles de consommateurs à gérer et à consigner les consentements.

Transparence et prise de décision automatisée

Puisque la confiance des consommateurs est essentielle au succès d'un système bancaire ouvert, la transparence est un thème récurrent dans le Rapport final[11]. Elle doit être présente dans la gouvernance[12], dans le processus d'accréditation[13] et dans le régime de responsabilité (y compris le processus de plainte et les règles entourant l'indemnisation en cas d'incident). Pour le Comité, « [l]es règles doivent être claires, simples et exécutoires de sorte que les consommateurs, peu importe leur niveau de littératie financière et leur vulnérabilité aux cyber menaces, puissent clairement apprécier qu'ils sont protégés pendant qu'ils utilisent le système »[14].

Reste à savoir si des exigences de transparence s'appliqueront à la prise de décision automatisée et à l'utilisation d'algorithmes. Dans son mémoire au Comité, le CPVP exhorte à porter une plus grande attention à l'analyse de mégadonnées et à l'utilisation de l'intelligence artificielle par les fintechs. Le CPVP a noté que le manque de transparence dans la façon dont les algorithmes automatisés sont employés dans le système bancaire ouvert pourrait compliquer la tâche de ceux qui souhaitent accéder à leurs renseignements et contester la conformité[15].

Ces algorithmes sont généralement exclusifs, et ils échapperaient probablement à la portée du cadre réglementaire. Toutefois, le droit des consommateurs d'être informés des décisions automatisées qui les touchent est une idée qui fait son chemin dans le domaine de la protection de la vie privée. Par exemple, le projet de loi n° 64 ajoutera une disposition à la loi québécoise visant le secteur privé qui obligera les entreprises qui prennent des décisions en se fondant uniquement sur le traitement automatisé de renseignements personnels à informer les personnes concernées des motifs et des principaux facteurs et paramètres qui ont mené à cette décision (entre autres)[16]. La LPVPC proposée, avant qu'elle ne soit abandonnée, contenait elle aussi une disposition obligeant les organisations à présenter un compte rendu général de l'utilisation de systèmes de décisions automatisées pour faire des prédictions, formuler des recommandations ou prendre des décisions qui pourraient avoir d'importantes répercussions sur les personnes concernées. Ces règles seront à surveiller, particulièrement pour les entreprises de gestion automatisée de placement et autres robots-conseillers.

Pouvoirs d'application

Dans son mémoire remis au Comité en février 2019, le CPVP demande que ses pouvoirs d'application soient accrus. Il souhaite notamment pouvoir rendre des ordonnances, imposer des amendes et procéder à des vérifications sans motif pour que les organisations demeurent assidues.

Le projet de loi n° 64 accordera à la Commission d'accès à l'information du Québec (la « **CAI** ») le pouvoir d'imposer des amendes allant jusqu'à 10 millions de dollars ou, s'il est plus élevé, jusqu'à un montant équivalent à 2 % du chiffre d'affaires mondial de l'entreprise. La LPVPC proposée autorisait elle aussi des amendes salées, pouvant dépasser les 10 millions de dollars ou 3 % du chiffre d'affaires mondial, en plus de donner au CPVP le pouvoir de rendre des « ordonnances de conformité ». Si le gouvernement fédéral dépose effectivement un nouveau projet de loi semblable à la LPVPC, des sanctions et des pouvoirs d'application du genre y seront sans doute prévus.

Conclusion

Si la législation fédérale en matière de protection de la vie privée a pris du retard par rapport aux règles québécoises, l'élaboration d'un système bancaire ouvert laisse présager l'arrivée d'une importante réforme. Les institutions financières et les fintechs ont intérêt à se tenir informées des changements législatifs, surtout si elles ont l'intention de participer à ce nouveau système.

Pour savoir comment bien vous préparer aux changements liés à l'instauration d'un système bancaire au Canada, communiquez avec un membre de notre groupe Services financiers ou de notre groupe Protection de la vie privée et des données.

[1][ps2id id='1' target='/] Rapport final, partie 12, « Grattage d'écran ».
[2][ps2id id='2' target='/]Les finances axées sur les clients : le futur des services financiers.
[3][ps2id id='3' target='/]Commissariat à la protection de la vie privée du Canada, Examen des mérites d'un système bancaire ouvert : Mémoire à l'intention du Ministère des Finances Canada.
[4][ps2id id='4' target='/]Rapport final, partie 5.4.
[5][ps2id id='5' target='/]Rapport final, partie 5.4.

[6][ps2id id='6' target='/] Projet de loi n° 64, article 112.
[7][ps2id id='7' target='/] LPRPDE, principe 4.7.
[8][ps2id id='8' target='/] *Banque Royale du Canada* c. *Trang*, 2016 CSC 50, paragr. 36.
[9][ps2id id='9' target='/]Rapport final, partie 7.1.
[10][ps2id id='10' target='/] LPRPDE, principe 4.3.6.
[11][ps2id id='11' target='/] Rapport final, partie 1.

[12][ps2id id='12' target='/] Rapport final, partie 6.
[13][ps2id id='13' target='/] Rapport final, partie 8.
[14][ps2id id='14' target='/] Rapport final, partie 7.1.
[15][ps2id id='15' target='/]Commissariat à la protection de la vie privée du Canada, Examen des mérites d'un système bancaire ouvert : Mémoire à l'intention du Ministère des Finances Canada, paragr. 14.

[16][ps2id id='16' target='/]Projet de loi n° 64, article 102.

par Darcy Ammerman, Mitch Koczerginski, Robbie Grant et Anthony Pallotta

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt obtenir des conseils juridiques précis.