

Mémoire du Mouvement Desjardins

**Projet de loi 82 - Loi concernant l'identité numérique nationale et
modifiant d'autres dispositions**

Commission des finances publiques

Janvier 2025

INTRODUCTION

Le Mouvement Desjardins est le 1^{er} groupe financier coopératif en Amérique, le 6^e au monde¹, et la 6^e institution financière au Canada avec un actif de 465 milliards \$. Comptant sur les compétences de plus de 55 000 employés et administrateurs, il a été nommé parmi les meilleurs employeurs 2024 au Canada par Mediacorp et Forbes. Pour répondre aux besoins diversifiés de ses 7,7 millions de membres et clients à travers le Canada, il offre une gamme complète de produits et services par l'entremise de son vaste réseau de points de service, ses plateformes virtuelles et ses filiales présentes à l'échelle du pays. Il exerce ses activités dans les domaines suivants : services aux particuliers et entreprises, gestion de patrimoine, assurance de personnes et assurance de dommages. Figurant parmi les institutions bancaires les plus solides au monde selon *The Banker*, Desjardins affiche des ratios de capital et des cotes de crédit parmi les meilleurs de l'industrie. Il se classe au 6^e rang des institutions financières les plus sécuritaires en Amérique du Nord et 33^e au monde, selon Global Finance².

En tant que groupe financier coopératif contribuant au développement des communautés, notre mission est d'accompagner nos membres et clients dans leur autonomie financière. Notre position distincte parmi les grandes institutions financières canadiennes et notre rôle d'acteur socio-économique de premier plan nous permettent d'apporter une perspective différente sur les politiques publiques.

C'est avec intérêt que nous avons pris connaissance de la publication par le ministre de la Cybersécurité et du Numérique du projet de loi 82, *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions*, présenté le 21 novembre 2024. D'entrée de jeu, nous saluons cette initiative du gouvernement qui permettra une transformation numérique bénéfique lors des interactions avec les citoyens, en faisant évoluer les pratiques et donnant lieu à une utilisation simplifiée et plus sécuritaire des services gouvernementaux. Ce mémoire vise à vous faire part de nos observations et commentaires quant aux impacts potentiels que pourrait avoir le projet de loi sur notre organisation et nos membres et clients.

L'ENGAGEMENT DE DESJARDINS ENVERS L'IDENTITÉ NUMÉRIQUE

L'engagement du Mouvement Desjardins envers l'identité numérique remonte à 2012 alors qu'il faisait partie des membres fondateurs du [Conseil canadien de l'identification et de l'authentification numériques \(CCIAN ou DIACC en anglais\)](#). En 2019, notre président, Guy Cormier, témoignait devant la Commission des finances publiques de l'Assemblée nationale le 21 novembre, et devant le Comité permanent de la sécurité publique de la Chambre des communes le 15 juillet, sur l'importance de la sécurité des renseignements personnels et la nécessité de repenser la notion d'identité numérique au Canada, considérant le fléau des vols de données chez de nombreuses entreprises, institutions financières et entités gouvernementales à travers

¹ Selon le [World Cooperative Monitor 2023](#)

² [Worlds-safest-banks-2023-global-100](#)

le monde. Il a notamment recommandé la formation d'un groupe de travail multipartite, composé minimalement de représentants des gouvernements, du secteur des services financiers et des assurances, du secteur des télécommunications, ainsi que des juristes et experts, afin de conseiller le gouvernement fédéral sur la manière :

- d'encadrer la gestion des données personnelles et de l'identité numérique et;
- d'adapter nos systèmes d'identification à l'ère numérique selon les meilleures pratiques dans le monde;

pour renforcer la protection des renseignements personnels des citoyens et mieux lutter contre la fraude et la cybercriminalité.

Un autre exemple de l'engagement du Mouvement Desjardins est sa participation à l'élaboration du [Livre blanc sur l'identité numérique](#), publié en mai 2023. Dans cet ouvrage, des entreprises privées au service de millions de personnes et d'entreprises du Québec présentent une vision partagée de l'identité numérique et de son intégration à la vie de tous les jours. L'objectif : favoriser l'émergence d'une compréhension commune, répondre à des questions de base de citoyens, consommateurs et dirigeants d'entreprises, susciter la collaboration entre les différents acteurs potentiellement impliqués dans l'implantation d'une identité numérique, et contribuer à créer un contexte favorable à son adoption.

Pour Desjardins, de multiples cas d'usage seraient possibles avec la consommation d'attestations numériques vérifiables, permettant d'obtenir les informations requises pour valider que la personne est bien celle qu'elle prétend être. Cela permettrait aussi, en fonction des attributs disponibles, d'accélérer certains processus au profit des utilisateurs, notamment en matière d'embauche de personnel et d'acquisition de produits pour les membres et clients (ex. ouverture d'un compte bancaire, octroi d'un prêt, d'une hypothèque ou d'une assurance, etc.). Nous vous invitons à lire le [Livre blanc](#) qui présente des exemples concrets de cas d'usage au quotidien. Le rehaussement de la sécurité résultant de la fiabilité des attestations numériques vérifiables et, à terme, la réduction des informations détenues par l'organisation sur les membres et clients seraient bénéfiques tant pour ces derniers que pour Desjardins et les autres entreprises de confiance participantes.

Enfin, nos investissements depuis les dernières années pour développer des façons de bénéficier des avantages de l'identité numérique chez Desjardins témoignent de notre engagement envers cette évolution nécessaire de la société. Aujourd'hui, notre utilisation de la technologie de vérification d'identité (hors attestations numériques vérifiables) permettant à une personne de s'ouvrir un compte 100 % en ligne, se fait grâce à deux solutions :

- [Service de vérification Interac](#) (SVI) pour la clientèle bancarisée au Canada (voir l'annexe);
- Vérification d'identité par document (VID) à distance à partir d'attestations numérisées (ex. permis de conduire, passeport) pour les clientèles jeunesse et nouveaux arrivants.

NOS OBSERVATIONS ET COMMENTAIRES

- **L'article 10.2** de la *Loi sur le ministère de la Cybersécurité et du Numérique* évoque la possibilité qu'une personne puisse utiliser l'identité numérique nationale afin de réaliser des interactions dans la collectivité, à l'aide d'attestations numériques gouvernementales dont elle détient le contrôle à partir d'une application où ces attestations sont déposées de façon sécurisée. Doit-on comprendre qu'une entreprise pourrait utiliser ces dites attestations afin d'identifier et/ou d'authentifier une personne et/ou de valider des informations à son égard? Nous aimerions obtenir des précisions sur la valeur juridique de l'identité numérique et la portée de son utilisation. Est-elle vouée à remplacer l'utilisation des identifiants gouvernementaux actuels à des fins d'authentification/identification?

De plus, nous aimerions connaître le niveau de sécurité de ces attestations. Aurons-nous la certitude, en tant qu'institution financière, que la personne qui nous présentera son attestation sera la bonne?

- **L'article 10.3** spécifie que l'utilisation de l'identité numérique nationale ne peut être imposée à une personne afin d'obtenir un service gouvernemental. Quels mécanismes d'identification et d'authentification seront proposés comme alternative? Il serait pertinent de le préciser dans le projet de loi ainsi que les conséquences, le cas échéant, pour une personne du refus d'utiliser l'identité numérique nationale et les attestations numériques gouvernementales qui y sont associées. A-t-on une assurance que les mécanismes actuels resteront en place tant et aussi longtemps que l'ensemble des citoyens n'auront pas adopté l'identité numérique?
- **L'article 10.4** confie au ministère de la Cybersécurité et du Numérique la responsabilité de la gouvernance et de la gestion centralisée de l'identité numérique nationale et qu'à ces fins, il peut :
 - « 1° définir, mettre en œuvre et appliquer un cadre de gouvernance des renseignements personnels dont la collecte, la communication et l'utilisation sont nécessaires pour l'identification et l'authentification des personnes;
 - 2° mettre en place des processus pour vérifier la cohérence et la qualité de ces renseignements. »

Il serait important que le projet de loi précise également la responsabilité de l'État en cas d'utilisation frauduleuse d'attestations numériques ou d'erreurs liées au traitement des renseignements personnels.

- **L'article 10.6**, au 1^{er} alinéa, attribue au ministère de la Cybersécurité et du Numérique la fonction d'agir comme source officielle de données numériques gouvernementales et prévoit, dans l'exercice de cette fonction, qu'il « *recueille, utilise ou communique des données numériques gouvernementales ou recueille auprès de toute personne des renseignements,*

incluant des renseignements personnels, lorsque cela est nécessaire. » (notre souligné). Même si les paragraphes 1 et 2 du 4^e alinéa de l'article 10.6 le spécifient, il serait pertinent de préciser sa portée dès le 1^{er} alinéa, en définissant le terme « auprès de toute personne » afin d'indiquer d'entrée de jeu que cela inclut autant les personnes physiques que morales. Cette précision pourrait avoir un impact sur les entreprises privées et une clarification pourrait être bénéfique pour un nombre important de participants. Est-ce que les entreprises privées devront communiquer des renseignements personnels sur leurs membres et clients?

- **L'article 10.7** prévoit ce que le registre de l'identité numérique nationale pourra notamment permettre. Au paragraphe 4 du 2^e alinéa, il est inscrit qu'une forme de traçabilité des accès au registre sera possible. Devons-nous comprendre que cette traçabilité sera également disponible au bénéfice des entreprises qui consulteront les données d'une personne, suivant son consentement, et ce, notamment afin de vérifier que l'entreprise a validé la donnée? Dans l'affirmative, le gouvernement devra prévoir un mécanisme pour permettre l'accès facile et sécuritaire aux données pour les employés de ces entreprises devant communiquer avec les organismes gouvernementaux.

Nous aimerions également que le projet de loi précise si le registre ou les nouveaux systèmes et infrastructures technologiques permettront l'hébergement de renseignements personnels à l'extérieur du Québec.

- **L'article 10.8** prévoit que le gouvernement peut déterminer les conditions et modalités d'une entente qu'un organisme public peut conclure dans le but de rendre interopérable l'identité numérique nationale avec les infrastructures et les systèmes de toute autre personne ou entité sur le plan local, régional, national ou international. Nous aimerions comprendre ce à quoi réfère le gouvernement quand il mentionne l'interopérabilité, autant par rapport à sa définition qu'à sa portée. Est-ce une interopérabilité entre gouvernements (Québec, Ontario, Colombie-Britannique, gouvernement fédéral, etc.) et/ou une interopérabilité avec les entreprises privées? Autrement dit, est-ce que les entreprises privées comme Desjardins pourraient être amenées à utiliser l'identité numérique nationale et ses attestations gouvernementales à des fins d'identification/d'authentification? Dans l'affirmative, nous aimerions :
 - Obtenir des précisions sur la portée des ententes qui pourraient être conclues avec des tiers, notamment concernant le contenu de celles-ci.
 - Savoir ce qu'il adviendra des partenaires de connexion présentement en opération (ex. Mon dossier de l'Agence du revenu du Canada, Service d'ouverture de session Interac utilisé par Revenu Québec – voir l'annexe). Le gouvernement doit évaluer si ces partenaires seront toujours fonctionnels à la suite des changements dans les infrastructures technologiques et si le processus d'authentification sous-jacent sera toujours d'actualité une fois l'identité numérique déployée.
 - Connaître s'il y aura d'autres projets de loi, de règlements ou d'ententes qui

toucheraient plus directement notre domaine d'activité. Est-ce que le service québécois d'identité numérique sera offert pour les institutions financières comme Desjardins qui pourraient consommer les attestations gouvernementales du Québec à l'intérieur de leur processus d'ouverture de compte bancaire selon les critères de connaissance du client (KYC³), d'acquisition de produits, de validation supplémentaire d'identité, etc.? Si oui, il sera important de nous impliquer en amont et prévoir des mécanismes pour partager de l'information entre les différentes institutions participantes et le gouvernement lors d'une usurpation d'identité ou d'un compte utilisé de manière illégitime, afin de communiquer rapidement avec les entités potentiellement touchées pour qu'elles prennent les mesures appropriées. Une solution similaire existe déjà avec le [Service de vérification Interac](#).

- **Les articles 10.9 et 10.10** prévoient que le gouvernement peut, par règlement :
 - Déterminer les modalités concernant la tenue du registre de l'identité numérique nationale.
 - Déterminer les normes de qualité des données numériques gouvernementales et, le cas échéant, des normes de protection particulières.
 - Préciser les données numériques gouvernementales, ayant des caractéristiques biométriques ou contenant des mesures biométriques, qui peuvent être utilisées, et ce, dans les cas et aux conditions qu'il détermine.
 - Prescrire toute autre mesure nécessaire à l'application du présent chapitre.
 - Prévoir des règles relatives à l'identification et à l'authentification des personnes.

Quels sont les mécanismes de contrôle prévus afin d'assurer la qualité des exigences des règlements gouvernementaux? Est-ce que le règlement est soumis à une expertise en matière de cybersécurité et/ou révisé par des tiers? Comment s'assure-t-on que tous les intervenants protègent adéquatement l'information? Nous aurions aimé voir dans le projet de loi une clause qui exige des audits et contrôles de la sécurité des systèmes impliqués dans le service d'identité numérique nationale. Par exemple, prévoir mandater une firme externe indépendante et reconnue en la matière pour auditer les mesures de sécurité et présenter un rapport incluant les correctifs mis en place de façon récurrente, et ce, afin d'éviter que l'un des organismes impliqués néglige de maintenir des mesures de sécurité adéquates.

- Enfin, dans plusieurs articles de la *Loi concernant le cadre juridique des technologies de l'information*, que le projet de loi 82 sur l'identité numérique viendra affecter, ce qui suit a été modifié : conformément aux normes ou standards « approuvés par un organisme reconnu visé à l'article 68 » par « généralement reconnus ». Serait-il possible de nous fournir plus de précisions sur ce qu'est une norme ou un standard qui est généralement reconnu ?

³ KYC = « Know Your Client » réfère au questionnaire de connaissance du client à compléter par les institutions financières et les preuves à fournir par la personne lors de l'ouverture d'un compte bancaire. Ce processus est encadré par les régulateurs du secteur financier dont le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).

NOS RECOMMANDATIONS AU GOUVERNEMENT

- Faire des consultations sur les nombreux règlements que le gouvernement peut définir suivant l'adoption du projet de loi 82 afin qu'ils tiennent compte des besoins des parties prenantes.
- Utiliser des technologies et procédures sophistiquées au niveau de la gestion du registre centralisé des données numériques gouvernementales comme le chiffrement. Puisque les données seront toutes conservées au même endroit, elles constitueront une cible d'intérêt pour les pirates informatiques contrairement à l'identité numérique décentralisée telle que proposée dans le [Livre blanc](#).
- Établir un cadre de gouvernance et mettre en place une Politique de confidentialité à l'intention des utilisateurs de l'identité numérique nationale précisant de manière transparente les pratiques d'utilisation, de collecte, de communication, de conservation et de destruction de renseignements personnels ainsi que les droits des individus afférents.
- Établir une saine gestion des consentements, notamment par la mise en place de mécanismes d'obtention et de retrait.
- Mettre en place des mesures de sécurité adéquates tenant compte de la sensibilité des renseignements personnels et faire auditer ces mesures par une firme externe spécialisée et indépendante.
- Encadrer, le cas échéant, l'hébergement de renseignements personnels hors du Québec pour assurer le respect des exigences de la loi 25.
- Définir un plan de continuité des affaires en cas de panne technique pour limiter les risques d'incident.
- Développer des standards clairs et des protocoles de collaboration entre les différents acteurs impliqués pour garantir le succès de l'identité numérique nationale.
- Porter un sérieux intérêt aux travaux et solutions numériques d'identification d'Interac, afin d'assurer l'interopérabilité entre les secteurs public et privé à l'échelle pancanadienne et favoriser l'adoption et le succès de l'écosystème québécois d'identité numérique.

CONCLUSION

Nous remercions la Commission des finances publiques de nous offrir l'occasion de commenter le projet de loi 82, *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions*. Nous sommes persuadés que les observations et recommandations du présent mémoire permettront de clarifier et bonifier l'encadrement de l'identité numérique nationale et sa mise en œuvre, au bénéfice de l'ensemble des Québécoises et Québécois. N'hésitez pas à communiquer avec nous pour approfondir certains éléments contenus dans ce mémoire. C'est avec plaisir que nous continuerons de contribuer activement aux travaux et consultations sur ce sujet d'intérêt pour les 7,7 millions de membres et clients du Mouvement Desjardins.

ANNEXE

1) Service de vérification Interac (identification)

- ▶ Ce service permet à la personne de **confirmer son identité pour accéder aux services numériques d'un fournisseur de services** (ex. Costco, Canadian Tire, Loto-Québec, Lobbyisme Québec, Sun Life, IA Groupe financier, etc.) en établissant une connexion sécurisée avec son institution financière (IF) participante.
- ▶ Le fournisseur de services indique les renseignements personnels nécessaires pour permettre l'identification, **la personne donne son consentement sur la communication de ces renseignements**, puis son IF les transmet de façon confidentielle et sécuritaire au fournisseur de services.
 - Avec la technologie utilisée, ni Interac, ni l'opérateur téléphonique/Internet, l'IF ou le fournisseur de services ne sait à quel service la personne accède et avec quel partenaire de connexion.
- ▶ **Les renseignements sont chiffrés** et transmis par le réseau d'Interac qui n'a pas accès à ces renseignements ni aux identifiants de connexion avec l'IF qui **ne sont pas stockés** dans l'application de Service de vérification Interac.
 - **Par exemple**, un membre de Desjardins qui veut consommer des services de Costco, le fait par le biais de sa connexion AccèsD et indique à Desjardins les informations à transmettre à Costco pour confirmer son identité. **Desjardins agit ici comme un fournisseur de données d'identité.**
 - Un client d'une banque qui veut devenir membre de Desjardins peut le faire par le biais de sa connexion à son application bancaire sécurisée et consent à ce que la banque transmette des données d'identité à Desjardins pour procéder à son ouverture de compte. **Desjardins agit ici comme un consommateur de données d'identité**, ce qui est possible depuis août 2023.
 - Grâce à ce service, **un membre de Desjardins pourrait éventuellement consentir à ce que l'Agence de revenu du Canada transmette certaines de ses données d'impôts à Desjardins afin de calculer/maximiser pour lui sa cotisation d'impôts** au lieu que le membre le fasse lui-même.

2) Service d'ouverture de session d'Interac (authentification)

- ▶ Ce service permet à une personne d'**accéder à des services gouvernementaux en ligne** (ex. Agence de revenu du Canada et Revenu Québec) **en utilisant ses identifiants de connexion (données d'authentification) avec son institution financière**, un partenaire de confiance dont le processus de vérification de l'identité est encadré par les critères KYC⁴, au lieu de créer/gérer de nouveaux noms d'utilisateur et mots de passe avec les différents services gouvernementaux.

⁴ KYC = « Know Your Client » réfère au questionnaire de connaissance du client à compléter par l'IF et les preuves à fournir par la personne lors de l'ouverture d'un compte bancaire. Ce processus est encadré par les régulateurs du secteur financier dont le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).