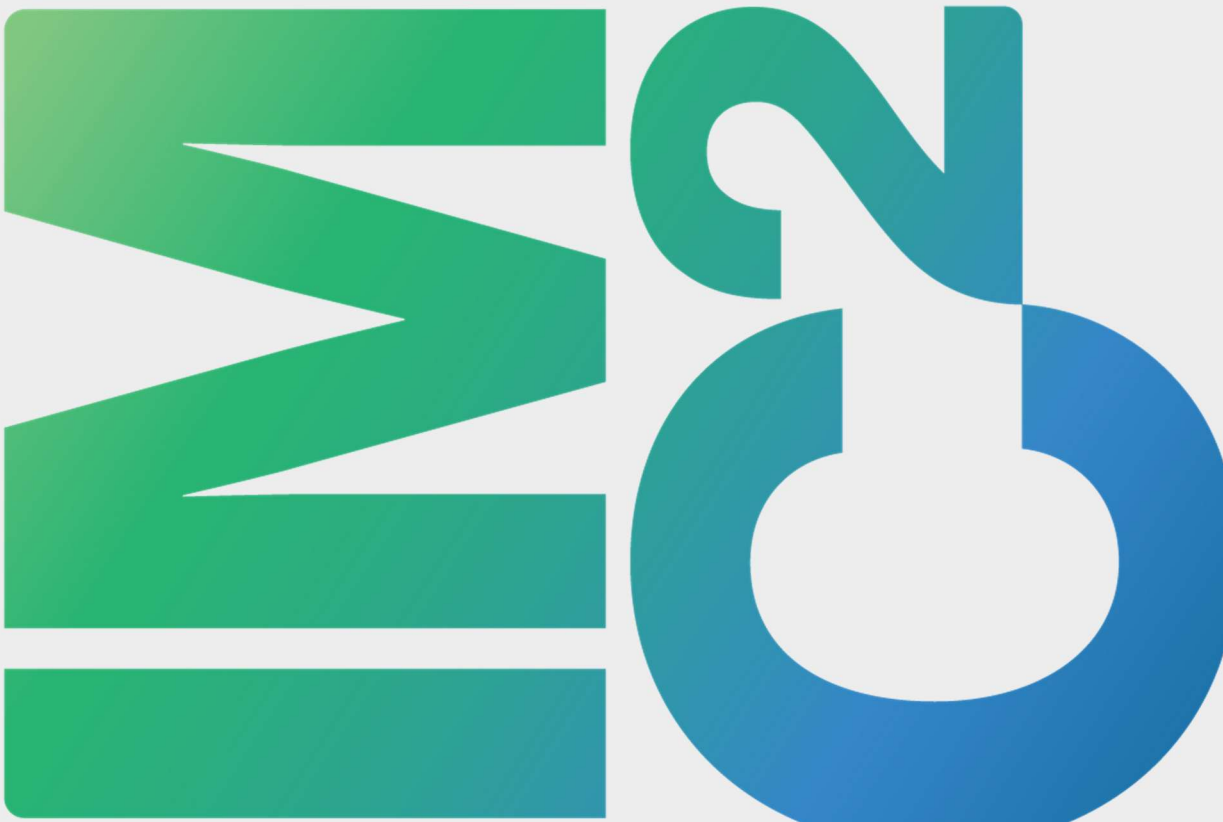
Institut
multidisciplinaire
en cybersécurité
et cyberrésilience

Travaillons ensemble à concevoir et concrétiser une société cyberrésiliente

Mémoire de l'IMC² dans le cadre des consultations particulières et auditions publiques sur le projet de loi n°82

Loi concernant l'identité numérique nationale et modifiant d'autres dispositions

Mémoire soumis à la Commission des finances publiques le 26 janvier 2025



Présenté par :

- **Frédéric Cuppens**, Directeur de l'IMC^2, professeur titulaire au Département de génie informatique et génie logiciel, Polytechnique Montréal
- **Benoît Dupont**, Directeur adjoint aux politiques publiques de l'IMC^2, professeur titulaire à l'École de criminologie, Université de Montréal
- **Marc Gervais**, Directeur exécutif de l'IMC^2

Avec la contribution de :

- **Nora Boulahia-Cuppens**, Directrice adjointe à la recherche de l'IMC^2, professeure titulaire au Département de génie informatique et génie logiciel, Polytechnique Montréal

À propos de l'IMC^2

L'Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC^2) fournit aux gouvernements, aux citoyens et aux entreprises du Québec et du Canada une expertise de premier plan par ses activités de recherche, la formation d'une relève aux compétences pertinentes, l'innovation et le partage de connaissances, et son soutien en matière de politiques publiques. Parmi les collaborateurs de l'organisation, on compte plus de quarante professeur·es et leurs équipes de recherche. L'IMC^2 est le fruit d'une collaboration entre Polytechnique Montréal, initiatrice du projet, en partenariat avec l'Université de Montréal et HEC Montréal.

1 Introduction

Le projet de loi 82, intitulé **"Loi concernant l'identité numérique nationale et modifiant d'autres dispositions"**, vise à établir un cadre légal pour la gouvernance de l'identité numérique au Québec. Il propose la création d'une infrastructure centralisée permettant aux citoyens d'accéder de manière sécurisée aux services gouvernementaux grâce à un système d'attestations numériques sous leur contrôle. Le ministre de la Cybersécurité et du Numérique se voit confier la gestion de cette identité numérique nationale.

Dans ce mémoire nous allons discuter des points suivants :

- Quels services pour une identité numérique nationale
- L'identification, l'authentification et l'autorisation
- Le registre de l'identité numérique
- Le consentement
- Le déploiement d'une identité numérique nationale

Enfin, nous conclurons ce mémoire.

2 Quels services pour une identité numérique nationale

Le projet de loi 82 marque une étape majeure vers une transformation numérique sécurisée des interactions entre l'État et les citoyens.

La création d'une identité numérique nationale au Québec va permettre le déploiement de trois services essentiels pour assurer la sécurité des accès aux services gouvernementaux. Ces trois services sont : l'identification, l'authentification et l'autorisation.

Nous commençons par discuter de ces trois fonctions en rappelant leur définition et en proposant ensuite plusieurs recommandations.

D'autres services comme la conservation des données ainsi que la traçabilité des données seront également étudiés en lien avec la création du registre de l'identité numérique nationale.

3 Identification numérique

L'identification numérique est le processus permettant d'attribuer et de reconnaître une identité unique à une entité dans un environnement numérique. Cette entité peut être une **personne physique**, une **personne morale**, voire un **objet connecté** (comme des dispositifs de l'internet des objets (IoT), des serveurs, ou des applications), afin de faciliter son interaction sécurisée dans un système ou un réseau.

Le projet de loi ne mentionne pas explicitement les entités qui se verront doter d'une identité numérique. Cependant, d'après la définition des données numériques gouvernementales données dans l'article 10.6,

on peut en déduire que les entités concernées sont les personnes physiques (correspondant aux données telles que le nom et les date et lieu de naissance d'une personne physique ainsi que le nom de ses parents), ainsi que les personnes morales (correspondant aux données telles que le nom et les coordonnées d'une personne morale ou d'une société de personnes).

Cependant, avec le développement de l'intelligence artificielle (IA) et de l'internet des objets (IoT), on peut anticiper le besoin de connexion, aux services gouvernementaux, par des objets connectés, tels que robots ou avatars, travaillant pour le compte de personnes physiques ou morales, mais disposant de leur propre identité numérique. Des normes existent déjà, telles que IEEE 802.1AR qui définit une structure standardisée pour attribuer une identité numérique unique, sécurisée et inviolable à chaque objet connecté.

Recommandation 1 : Pour les besoins d'identification futurs, nous suggérons de ne pas limiter l'identification aux personnes physiques et morales mais d'inclure également la possibilité de créer une identité numérique nationale pour les objets connectés.

4 Authentification

L'authentification est le processus de vérification de l'identité déclarée d'une entité possédant une identité numérique pour s'assurer qu'elle est bien celle qu'elle prétend être. Ce processus repose sur la validation de preuves ou de justificatifs fournis par l'entité lors de l'accès à un système ou un service.
L'authentification est dite multi-facteur lorsqu'on combine plusieurs facteurs pour renforcer la sécurité, par exemple : un mot de passe (quelque chose que vous savez) + une validation via un téléphone intelligent (quelque chose que vous possédez).

Recommandation 2 : L'authentification sécurisée est un service clé que permet d'apporter l'identité numérique. Le projet de loi (ou sinon la définition du règlement prévu dans le texte du projet de loi) devrait préciser les obligations à respecter en termes d'usage d'authentification multi-facteurs (MFA).

Recommandation 3 : Le règlement devrait également prévoir l'abolition de l'usage des « questions secrètes » dans le processus d'authentification telles que « Quel est le prénom de votre mère » qui reposent sur la collecte de données personnelles. Ces questions secrètes deviennent inutiles dès lors qu'une identité numérique est créée.

Recommandation 4 : L'usage d'une authentification reposant sur des données biométriques nécessite la collecte de données personnelles. Elle ne devrait être envisagée que lorsque que cela est strictement nécessaire. L'utilisation de mot de passe à usage unique devrait être préférée.

5 Autorisation

L'autorisation est le processus qui détermine si une entité possédant une identité numérique a le droit d'accéder à une ressource, d'effectuer une action spécifique ou d'utiliser un service.

L'autorisation intervient après l'identification et l'authentification. Une fois que l'identité d'une entité est vérifiée, le système évalue les autorisations associées à cette identité. Ainsi, l'accès à certains services peut n'être autorisé que si l'usager satisfait certaines conditions, par exemple liées à l'âge ou la situation professionnelle de la personne. Pour vérifier que la personne physique ou morale satisfait ces conditions, il est nécessaire de collecter des données personnelles de façon sécurisée.

Recommandation 5 : Le projet de loi devrait clairement prévoir le besoin de collecter certaines données personnelles pour gérer les autorisations d'accès aux services gouvernementaux.

6 Registre de l'identité numérique

Le projet de loi prévoit la création d'un registre de l'identité numérique pour collecter, de façon centralisée, certaines données personnelles. Le projet de loi indique qu'il est de la responsabilité du Ministre de la Cybersécurité et du Numérique d'assurer la conservation et la traçabilité des données contenues dans ce registre.

Recommandation 6 : Le projet de loi devrait préciser davantage dans quel but ce registre est créé ainsi que les données qui seront concernées par ce registre.

Recommandation 6.1 : Les données personnelles ne peuvent pas être collectées sans préciser la finalité. De notre point de vue, les données collectés dans ce registre devraient être limitées aux besoins du service d'identification, d'authentification et d'autorisation. Tous les services autres que l'identification, l'authentification et l'autorisation ne nous semblent pas relever directement d'un projet de loi sur l'identité numérique. Les pouvoirs réglementaires associés aux articles suivants nous paraissent ainsi insuffisamment justifiés : Article 10.6, alinéa 4, paragraphe 3°, article 10.7, alinéa 2, paragraphe 5° et article 10.9, paragraphe 4°.

Recommandation 6.2 : Le projet de loi devrait préciser que le ministre doit non seulement assurer la qualité et la cohérence de ces données, mais aussi leur confidentialité, leur intégrité et leur disponibilité.

7 Consentement

Le consentement est l'approbation explicite et éclairée donnée par une personne ou une entité pour permettre un traitement spécifique de ses données personnelles, une action ou une interaction. Dans les environnements numériques, le consentement est une condition préalable essentielle pour respecter la

confidentialité et les réglementations légales, comme la loi 25 ou le RGPD européen (Règlement Général sur la Protection des Données).

Recommandation 7 : Les données personnelles collectées dans le registre de l'identité numérique devraient être soumises au consentement explicite des personnes physiques et morales. De plus, les modalités d'accès et de rectifications des données, ainsi que de retrait du consentement devraient être définies.

8 Déploiement d'une identité numérique nationale

Le déploiement d'une identité numérique nationale va nécessiter des ressources techniques et organisationnelles très importantes. Par ailleurs, le secteur privé, gère déjà des systèmes d'identification et d'authentification pour l'accès à certains services (financiers par exemple), et pourrait aussi offrir des services en soutien au registre de l'identité numérique nationale.

Recommandation 8 : Le projet de loi devrait préciser quels seront les mécanismes de gouvernance et le modèle de partenariat prévu avec le secteur privé.

Recommandation 9 : Dans certains pays, les outils communiquent ou sont partagés, alors que dans d'autres, ils sont exclusifs. La nature des interactions prévues pourrait faire l'objet de plus grandes précisions dans la Loi.

Recommandation 10 : Par ailleurs, l'article 5.2 (p. 5) mentionne que l'une des motivations à la Loi est de favoriser la mutualisation (centralisation) et l'optimisation des structures. Cependant, la notion de cyber-résilience, qui exige parfois des mesures non-optimisées pour garantir la robustesse ou un rétablissement rapide grâce à des ressources excédentaires, devrait aussi figurer comme l'un des objectifs ultimes de la Loi. Une vigilance toute particulière doit être apportée à la nature centralisée proposée dans ce projet de loi, car il constitue potentiellement un point unique de défaillance pour l'ensemble des services gouvernementaux.

Recommandation 11 : On peut également observer que l'intelligence artificielle (IA) n'est pas mentionnée dans la loi (à part dans une mention de l'interdiction du profilage) : il serait pertinent d'inclure des dispositions qui préciseraient les conditions et paramètres d'utilisation de l'IA, ainsi que sa surveillance, en lien avec le déploiement d'une identité numérique nationale.

Recommandation 12 : Enfin, la question de l'articulation avec une identité numérique Canadienne n'est pas mentionnée (si ce n'est par une interopérabilité), et mériterait peut-être plus de détails.

9 Conclusion

Le projet de loi inclut les articles 5.2 et 5.3 qui donne au ministre la responsabilité de développer et de soumettre au gouvernement une vision globale des infrastructures et des services de télécommunications jugés utiles ou essentiels pour la conduite des affaires de l'État. Les deux articles sont très importants, et soulèvent plusieurs questionnements, par exemple comment faire respecter les obligations pour les opérateurs privés de systèmes ou d'infrastructures essentielles en cas d'atteinte à la sécurité. Nous ne les avons pas commentés dans ce mémoire car ils ne nous semblent pas relever d'un projet de loi sur l'identité numérique nationale. **Ils devraient faire l'objet d'un projet de loi séparé sur les responsabilités du MCN en matière de supervision des infrastructures essentielles et des services de télécommunications.**

En conclusion, la création et le déploiement d'une identité numérique nationale représentent un défi majeur pour le Québec. L'IMC^2 soutient complètement cette démarche et propose ses services au Ministère de la Cybersécurité et du Numérique pour aider, conseiller et contribuer à ce projet.