L'identité numérique auto-souveraine : Principe clé de l'identité numérique nationale

Mémoire présenté 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*

Document développé par :

Institut de gouvernance numérique (IGN)

Chaire de recherche sur les contrats intelligents et la chaîne de blocs – Chambre des notaires du Québec (Université Laval)

Chaire de recherche industrielle T-RIZE en application de systèmes de chaîne de blocs durables et pratiques (École de technologie supérieure)

28 janvier 2025

1. PRÉSENTATION DES INTERVENANTS

Institut de gouvernance numérique

L'Institut de gouvernance numérique (IGN) a pour mission de soutenir une transformation numérique profitable, durable et efficiente des organisations publiques et privées grâce à des services de sensibilisation, de formation, d'accompagnement et de financement en gestion collaborative ; le tout ancré dans les besoins et les réalités du terrain. En facilitant l'implantation dans les organisations d'une gouvernance dont les bases sont la transparence, la participation et la collaboration, IGN facilite une transformation numérique profitable, durable et efficiente.

Chaire de recherche sur les contrats intelligents et la chaîne de blocs – Chambre des notaires du Québec (Université Laval)

La mission de la Chaire est d'étudier les aspects juridiques reliés aux contrats intelligents et à la chaîne de blocs en droit québécois, de proposer une réflexion critique sur les enjeux relatifs à l'introduction des nouvelles technologies dans le monde juridique, notamment en matière de protection du public et d'accès accru à la justice, et d'accompagner le notariat québécois dans son exercice de transformation numérique.

Chaire de recherche industrielle T-RIZE en application de systèmes de chaîne de blocs durables et pratiques (École de technologie supérieure)

La Chaire de recherche T-RIZE en application de systèmes de chaîne de blocs durables et pratiques a pour objectif de sortir les applications liées aux chaînes de blocs et à la numérisation d'actifs des domaines où elles sont utilisées traditionnellement, tels que la cryptomonnaie et les jetons non fongibles (NFT) pour les arts numériques.

L'équipe du professeur Kaiwen Zhang s'attache à démocratiser cette technologie en travaillant à la conception d'innovations techniques qui permettront de créer des chaînes moins énergivores, tout en améliorant leur flexibilité, leur interopérabilité et leur sécurité.

2. MISE EN CONTEXTE – COLLABORATION ANTÉRIEURE ENTRE LES INTERVENANTS ET LIVRE BLANC

En novembre 2019, l'IGN a produit un livre blanc sur le potentiel des registres distribués et les chaînes de blocs au Québec auquel ont collaboré les titulaires des deux chaires citées précédemment, soit les professeurs Charlaine Bouchard (Université Laval) et Kaiwen Zhang (ETS).

Ce document, intitulé *Registres distribués, l'évolution de la chaîne de blocs : Impacts, enjeux et potentiels pour le Québec*, dont les principes sont aussi valides aujourd'hui qu'ils l'étaient au moment de la publication est le résultat de travaux menés par un comité composé d'universitaires, d'entrepreneurs, d'avocats et d'administrateurs publics.

L'Autorité des marchés financiers, Québec Blockchain, Catallaxy (une filiale de Raymond Chabot Grant Thornton), Bitfarms, l'Université Laval, l'École de technologie supérieure ainsi que La Capitale ont aussi contribué à l'exercice. L'information contenue dans ce livre blanc est le fruit d'entrevues réalisées avec des experts, des entrepreneurs, des chercheurs et une revue de documentation constituée d'études, de sondages et de documents d'institutions tant publiques que gouvernementales, du Canada comme de l'étranger.

Le Scientifique en chef du Québec, Hydro-Québec, le ministère de l'Économie et de l'Innovation du Québec, le ministère des Finances du Québec, Finance Montréal et le Hub Saguenay–Lac-Saint-Jean ont rendu possible la préparation de ce livre blanc par leurs contributions financières respectives.

Ainsi, le mémoire qui suit s'inscrit en parfaite continuité avec ce livre blanc et, par conséquent, nous proposons la modification de certaines dispositions du projet de loi pour y inscrire certains principes qui nous apparaissent fondamentaux pour réduire les risques et surtout redonner aux citoyens la confiance et les moyens de gérer eux-mêmes l'accès à leurs informations personnelles.

3. L'IDENTITÉ NUMÉRIQUE AUTO-SOUVERAINE – UN PRINCIPE CLÉ DEVANT ÊTRE AU CŒUR DE L'IDENTITÉ NUMÉRIQUE NATIONALE

3.1. Qu'est-ce que l'identité numérique auto-souveraine ?

L'identité numérique auto-souveraine (Self-Sovereign Identity, SSI) offre un cadre novateur qui place l'individu au centre de la gestion de son identité numérique[1], tout en s'appuyant sur des technologies décentralisées et des standards ouverts pour garantir sécurité, interopérabilité et autonomie[2]. Contrairement aux modèles centralisés ou fédérés, qui concentrent les données dans des bases contrôlées par des tiers, la SSI propose une approche distribuée, où chaque individu possède et contrôle directement ses identifiants et ses informations personnelles. Cette approche s'articule autour de principes fondamentaux qui correspondent aux valeurs de protection de la vie privée et d'autodétermination informationnelle[3].

3.2. Grands principes de l'identité numérique auto-souveraine

3.2.1. Le contrôle individuel

Le contrôle individuel constitue le fondement de l'identité numérique auto-souveraine.

Il renvoie à la possibilité pour chaque personne de disposer des pouvoirs décisionnels sur la création, l'accès et le retrait d'attributs relatifs à son identité[4]. En ce sens, chaque participant à un système d'identité numérique auto-souveraine détient des identifiants sous forme d'attestations numériques vérifiables qu'il peut partager de manière sélective et sécurisée[5].

Selon la Sovrin Foundation, une identité numérique véritablement auto-souveraine permet aux citoyens de gérer eux-mêmes leurs informations sans intervention d'intermédiaires, tout en assurant une protection accrue contre les abus[6]. Ce contrôle est renforcé par les technologies cryptographiques, qui garantissent la confidentialité des données partagées.

---

[1] Jessica Eynard, « L'identité numérique autosouveraine, objet juridique non identifié » dans Jessica Eynard & Giorgia Macilotti, dir, *Identité numérique en construction : Quels Enjeux et quels modèles ?*, Collection Rencontres européennes 33, Bruxelles, Bruylant, 2024 35.

[2] Drummond Reed & Oskar van Deventer, « The basic building blocks of SSI » dans Alex Preukschat & Drummond Reed, dir, *Self-Sover Identity*, Manning Publications, 2021 21, Google-Books-ID: BfQ1EAAAQBAJ.

[3] Eynard, *supra* note 1.

[4] Alexander Mühle et al, « A survey on essential components of a self-sovereign identity » (2018) 30 Comput Sci Rev 80-86.

[5] Kevin Wittek et al, « An SSI Based System for Incentivized and SelfDetermined Customer-to-Business Data Sharing in a Local Economy Context » (2020) 2020 IEEE Eur Technol Eng Manag Summit E-TEMS 1-5.

[6] https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

3.2.2. Minimisation des données

L'un des principes fondamentaux du cadre SSI est la minimisation des données. Cette approche repose sur la divulgation sélective et limitée des informations personnelles, par exemple en prouvant qu'une personne est majeure sans révéler sa date de naissance complète. Ce principe est rendu possible grâce à des outils tels que les preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs), qui valident des assertions sans révéler les données sous-jacentes. Ces techniques protègent la vie privée tout en respectant les exigences d'intégrité et de fiabilité des informations échangées.

3.2.3. Décentralisation et interopérabilité

L'architecture de la SSI s'appuie également sur la décentralisation et l'interopérabilité, en utilisant des registres distribués, souvent sous forme de chaînes de blocs, pour créer une infrastructure résiliente et transparente[7].

Les standards ouverts, tels que les Decentralized Identifiers (DID) et les Verifiable Credentials (VC) promus par le W3C[8], permettent une reconnaissance et une utilisation universelle des identités numériques. Ces standards assurent une interopérabilité entre les différents écosystèmes numériques, facilitant ainsi les interactions entre citoyens, institutions publiques et entités privées.

L'utilisation de registres distribués garantit par ailleurs que les identifiants ne sont pas stockés dans des bases centralisées, limitant ainsi les risques liés à un point de défaillance unique.

3.2.4. Transparence et traçabilité

La transparence et la traçabilité, enfin, jouent un rôle déterminant dans le renforcement de la confiance dans le cadre de la SSI. Chaque interaction liée à l'accès ou à l'utilisation des données est enregistrée de manière immuable, permettant aux citoyens de vérifier en temps réel qui a accédé à leurs informations, à quelles fins et dans quel contexte. Ces registres d'accès, combinés à des mécanismes d'audit rigoureux, assurent une conformité avec les exigences réglementaires et renforcent la responsabilisation des parties prenantes.

[7] A Fraser & S Schneider, « On the role of blockchain for self-sovereign identity » (2022) 2022:8 IET Conf Proc 17-21; IndoAI Technologies P Ltd, Pune, Maharashtra, Pune & Vivek Gujar, « IDENTITY MANAGEMENT, SSI AND BLOCKCHAIN: A REVIEW » (2023) 08:07 Int J Eng Appl Sci Technol 38-45.
[8] https://www.w3.org/TR/

3.3. Un chemin pour une identité numérique nationale respectueuse des principes SSI

L'objectif ultime du cadre SSI, donner le plein contrôle sur son identité à l'individu dans un environnement totalement décentralisé peut parfois entrer en tension avec la réalité des États, au sein desquels, la gestion de l'identité participe à la fois de la reconnaissance juridique du citoyen et de l'exercice de prérogatives gouvernementales, notamment celles liées à la sécurité publique.

Au reste, dans un état démocratique comme le Québec, il est difficilement envisageable d'établir un cadre dans lequel l'identité numérique du citoyen est la propriété du gouvernement et fait l'objet d'une centralisation opaque. Entre deux extrêmes – une décentralisation complète et une centralisation rigide – se dessine une voie intermédiaire : la fédération d'identité.

La fédération d'identité est un modèle conceptuel qui permet de concilier les impératifs gouvernementaux de gestion de l'identité avec la reconnaissance d'une plus grande autonomie des citoyens dans la gestion de leurs données[9].

La fédération d'identité repose sur une architecture décentralisée (ou intégrée) et modulaire, dans laquelle plusieurs entités (par exemple, des ministères, des agences publiques ou des organismes autorisés) agissent en tant que fournisseurs d'identité, tout en respectant des standards communs et en assurant une interopérabilité entre leurs systèmes.

Dans le cadre du projet d'identité numérique nationale et de la transformation numérique gouvernementale, ce modèle, ainsi que les concepts associés nous semblent être des repères utiles.

4. ANALYSE DU PROJET D'IDENTITÉ NUMÉRIQUE DÉPOSÉ PAR LE GOUVERNEMENT DU QUÉBEC ET FORMULATION DE RECOMMANDATIONS

Nous procéderons à l'analyse du projet de loi n° 82, *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions*, sous deux angles :

- L'identité numérique nationale centrée sur le citoyen ; et
- L'identité numérique nationale ancrée dans un cadre de gouvernance intégré et transparent.

4.1. Une identité numérique centrée sur le citoyen

[9] Jesus Carretero et al, « Federated Identity Architecture of the European eID System » (2018) 6 IEEE Access 75302-75326.

Le projet de loi 82 définit une « identité numérique nationale », qui serait un « ensemble des moyens dont dispose l'État pour garantir à toute personne un accès sécurisé aux prestations électroniques de services gouvernementales et lui permettre d'avoir un niveau de confiance élevé lors de ses interactions avec les organismes publics » (Art. 6 PL instituant 10,2 Loi sur MCN).

L'identité numérique est donc abordée, principalement, à travers une finalité, un acteur clé et des bénéficiaires. Dans les alinéas suivants, des précisions sont faites sur les autres usages et sur les modalités pratiques possibles de l'identité numérique. Le projet de loi s'inscrit dans un cadre d'initiatives gouvernementales plus vaste, qui ont pour dessein la transformation numérique de l'administration. Ce contexte pourrait être une explication éventuelle de l'approche téléologique, orientée vers la prestation de services numériques au citoyen, retenue dans le projet de loi. Au reste, une telle approche risque, en plaçant la prestation de services numérique au cœur de la démarche, de réduire l'attention accordée intrinsèquement au phénomène de l'identité dans son rapport avec son titulaire, ici le citoyen.

En effet, qu'on agisse dans et en dehors de l'univers numérique, il est nécessaire pour entrer dans une relation de confiance avec une autre personne d'établir qui nous sommes. Ce « qui nous sommes », notre identité, est composé d'un ensemble d'attributs, qui peuvent être objectifs, subjectifs, stables, évolutifs, relationnels, etc. En effet le critère de détermination des attributs peut varier et, dans la littérature académique, il existe différentes définitions du concept et des attributs de l'identité[10].

Dans ce contexte, au milieu des incertitudes, les États contemporains ont mis en place des cadres juridiques et institutionnels qui permettent de reconnaître certains attributs fondamentaux aux personnes et de les distinguer d'autres personnes. Ainsi, dans un État donné, des émanations de la puissance publique, suivant des procédures légalement établies, vont collecter de l'information sur une personne, produire un document juridique attestant de l'existence de ces informations et produire un document qui permet au titulaire de l'identité de s'en prévaloir.

Au Québec par exemple, le Directeur de l'État civil est chargé de collecter certaines informations sur les nouveau-nés à travers la déclaration de naissance, qu'il utilise pour dresser un acte de naissance, dont il fournit une copie ou un certificat qui permet au titulaire de se prévaloir d'une identité légale et des droits afférents.

Dans certains pays (France, Estonie, Singapour, etc.), la loi institue une carte nationale d'identité, qui présente pour objectif spécifique de permettre aux citoyens d'un certain âge de prouver leur identité. À cette fin particulière, une procédure est mise en place pour collecter des données déterminées, dresser un acte sanctionnant la collecte de ces données et émettre un justificatif, en l'occurrence la carte nationale d'identité.

[10] *Rapport d'information déposé en application de l'article 145 du Règlement par la mission d'information commune sur l'identité numérique*, par Marietta Karamanli, Christine Hennion & Jean-Michel Mis, 3190, France, Assemblée nationale de France.

En France, cette carte nationale d'identité sert notamment de fondement à l'identité numérique proposée par l'État. Concrètement, l'identité numérique citoyenne d'un français, correspond à l'émission d'un justificatif numérique sur la base d'un document d'identité préexistant, la carte nationale d'identité ou le permis de conduire. Le projet d'identité numérique dans ce contexte n'a pas eu pour conséquence de créer un nouveau document d'identification et correspond uniquement à une transposition dans l'univers numérique de formes d'identification officielles déjà juridiquement et socialement acceptées.

Dans le contexte québécois, il existe une diversité de documents officiels comprenant des informations sur le titulaire. Qu'on pense à la carte d'assurance maladie, au permis de conduire, au certificat de naissance ou à l'avis de cotisation, différents documents, émis par divers ministères et organismes du gouvernement contiennent des informations, pouvant être considérées comme des attributs du titulaire. Pour autant, à la différence de l'exemple de la France précitée, il n'existe pas à notre connaissance, dans les lois québécoises, un document officiel dont l'objectif primaire et unique est de prouver l'identité d'une personne.

Sans vouloir préjuger des circonstances et des raisons entourant cet état de fait, il nous semble important de souligner son existence et par conséquent d'ouvrir le débat sur l'opportunité du maintien d'un système équivalent en ligne. Il est possible de dériver une identité numérique à partir des documents officiels couramment utilisés au Québec et, si on devait faire un choix différent, il serait souhaitable d'avoir un débat public pour entendre la voix des citoyens sur la question.

Recommandation 1 : Tenir un débat public sur l'opportunité d'un titre d'identification nouveau ou dériver l'identité numérique sur la base d'une pluralité de documents d'identité.

Dans l'état actuel des choses, le Registre d'attributs d'identité gouvernemental (RAIG) agit comme source de l'identification des personnes, afin d'assurer l'accès à des prestations électroniques de service gouvernementales. Ce registre a été institué par décret pour la mise en œuvre du Service d'authentification gouvernementale (SAG) et les données qu'il comprend proviennent essentiellement de la Régie de l'assurance maladie du Québec (RAMQ), incluant notamment le numéro d'assurance maladie et le numéro d'assurance sociale et son historique.

Le décret créant le RAIG mentionne clairement, dans son 5^{e} attendu, que l'utilisation et la communication de ces données sont soumises au consentement des personnes. L'article 40 PL82 prévoit que le RAIG devient le registre de l'identité numérique nationale, tel que défini à l'article 6 PL82 (10,7).

La qualification de ce registre en tant que système de dépôt et de communication des données numériques gouvernementales soulève certains enjeux sur le modèle de gouvernance de l'identité numérique nationale, qui seront abordés plus loin dans ce mémoire.

À ce stade-ci, nous nous questionnons sérieusement sur la place du consentement du citoyen relativement à la mobilité des données nécessaires à la mise en œuvre de ce registre. L'article 6 (10,3) du projet de loi semble limiter le caractère facultatif de l'identité numérique nationale à la question de l'obtention de prestations de service gouvernementales.

Aucun article ne précise toutefois le caractère facultatif de l'existence même de l'identité numérique pour un individu ni l'obligation pour l'organisme en charge de mettre en œuvre le registre d'identité numérique nationale de recueillir le consentement préalable du citoyen avant de collecter ou de communiquer ses données.

En conséquence, la mise en œuvre d'une identité numérique associée à chaque citoyen deviendrait systématique et permettrait, nonobstant le caractère facultatif de l'utilisation de l'identité numérique par le citoyen, son utilisation par les organismes publics.

Recommandation 2 : Insérer dans l'article 6 PL82, avant le 10.2, l'article suivant « la communication et l'utilisation de l'identité numérique du citoyen par le gouvernement sont soumises à son consentement ».

L'identité numérique gouvernementale joue un rôle déterminant dans le projet de transformation numérique gouvernementale. Il est toutefois nécessaire, en dépit des nombreuses connexions qui peuvent être établies, de préciser qu'il s'agit de deux choses différentes.

Traditionnellement, la gestion de l'identité officielle d'une personne fait partie intégrante des fonctions souveraines de l'État. Au reste, cette association de l'identité avec l'exercice de la souveraineté de l'État coexiste avec un autre impératif, de l'ordre de l'obligation des États, qui est la reconnaissance juridique du citoyen.

Le décalage entre le développement rapide de l'utilisation des outils numériques et la fourniture dans cet espace de justificatifs d'identité de source officielle a créé les conditions d'émergence de fournisseurs d'identité privés.

En l'absence d'alternatives publiques, les internautes ont le choix entre refuser d'effectuer certaines prestations nécessitant de prouver son existence en ligne ou recourir à des prestataires privées, notamment les banques, pour prouver leur identité. Cet état de fait, au regard de la place centrale qu'occupent actuellement les interactions avec le numérique, appelle une réaction des États, qui doivent continuer, en dépit du lieu, d'offrir les services liés à la gestion de l'identité des personnes.

L'enjeu ici est très précis, il faut offrir au citoyen des moyens gouvernementaux de prouver qui il est en ligne. À l'instar du monde physique, le « qui il est » s'entend, pour les documents officiels, d'un ensemble d'attributs déterminés dans un cadre juridique clair, qui permettent d'établir avec certitude sa singularité.

Cette approche de l'identité numérique ressort clairement dans le règlement européen couvrant l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS 2.0). Ce règlement, à la suite du règlement eIDAS, établit un cadre juridique harmonisé permettant aux citoyens de prouver leur identité en ligne à travers des moyens électroniques reconnus et interopérables dans tous les États membres de l'Union européenne[11]. Il impose des standards élevés en matière de sécurité, d'interopérabilité et de reconnaissance mutuelle des systèmes d'identité, tout en garantissant la protection des données personnelles.

La mise à disposition de prestations de services gouvernementales, lorsque ces prestations nécessitent un niveau de confiance élevé, peut être facilitée par l'utilisation de l'identité numérique. Il demeure toutefois que l'identité ne devrait pas s'expliquer principalement par la nécessité d'offrir des prestations bonifiées au citoyen. Elle constitue, même dans l'univers numérique, un ensemble d'attributs désignés dans un cadre juridique précis, qui permet de distinguer une personne et de la reconnaître juridiquement.

Comme indiqué dans le projet de loi, une diversité de moyens peut contribuer à la mise en œuvre de l'identité numérique et cette identité permet d'accéder à une pluralité de services, dans et à l'extérieur du monde numérique. Tous ces éléments contextuels sont importants et présentent un intérêt dans une loi qui érige le cadre juridique et institutionnel de l'identité numérique. Ils n'effacent toutefois pas le besoin de définir ce que constitue intrinsèquement cette identité.

Recommandation 3 : Insérer un article avant l'article 10.2 : « L'identité numérique citoyenne est un ensemble d'attributs associés à une personne, enregistrés sous forme numérique, qui permettent de le distinguer d'autres personnes de façon unique et non équivoque ».

4.2. Une identité numérique nationale avec un cadre de gouvernance intégré et transparent

Le projet de loi 82 propose une architecture de gouvernance et d'opérationnalisation de l'identité numérique nationale qui, de prime abord, peut sembler hypercentralisée. Dans sa mouture actuelle, il confie au ministre de la Cybersécurité et du Numérique (MCN) la responsabilité de la gouvernance et de la gestion centralisée de l'identité numérique nationale. Le ministre détermine en ce sens par règlement les règles relatives à l'identification et à l'authentification des personnes. Il est ainsi responsable du cadre de gouvernance de l'identité numérique gouvernementale.

[11] https://www.european-digital-identity-regulation.com/

Par ailleurs, le MCN est désigné comme source officielle des données numériques gouvernementales en matière d'identité numérique. Il devient, par conséquent, gestionnaire des données numériques gouvernementales collectées à cet effet et responsable de l'application des règles désignées dans le cadre de gouvernance préétablie. Dans l'état actuel des choses, il existe une diversité d'organismes publics qui collectent des renseignements personnels qui pourraient être affectés par cette mesure, étant entendu que la liste des renseignements personnels figurant dans le PL peut être étendue par règlement (Art 6. PL, Art. 10. 6 MCN). Cette situation soulève certains enjeux sur l'autonomie des organismes publics et des conséquences sur l'imputabilité.

Aussi, l'aspect technique de la mise en œuvre du registre de l'identité numérique nationale sera très probablement sous sa responsabilité. Le projet de loi, dans son article 1 et suivants, prévoit en effet un élargissement de l'offre de services du ministre, qui en lieu et place d'offrir des services en « infrastructures technologiques et en systèmes de soutien communs », offre dorénavant des services en « ressources informationnelles ». Le PL prévoit aussi que « le ministre développe et exploite, à des fins non commerciales, un réseau d'infrastructures de connectivité en lien avec les services de télécommunications qu'il fournit » (Art. 3).

En bout de course, dans le cadre de l'identité numérique, le MCN serait à la fois responsable de la gouvernance, de la gestion et de l'opérationnalisation technique. Si le projet de loi est adopté, éventuellement, dans le futur, pour d'autres projets en ressources informationnelles, cette situation risque de se présenter à nouveau. Comme nous l'avons souligné, cela crée des enjeux d'autonomie des différents ministères et organismes du gouvernement et a des conséquences sur l'imputabilité. Dans le cadre de la transformation numérique gouvernementale, il est probable que cette approche permet d'atteindre un certain niveau d'efficience. Au reste, pour l'identité numérique, afin d'offrir un cadre transparent, clair et renforçant la confiance des citoyens, une approche différente est nécessaire.

Recommandation 4 : Établir une séparation claire entre la définition des politiques et la mise en œuvre opérationnelle des initiatives gouvernementales. Pour l'identité numérique, conserver le modèle de centralisation pour la détermination des politiques et assurer une mise en œuvre concertée et décentralisée par les différents ministères et organismes de l'État.

Dans la même logique de différenciation entre les rôles et de répartition moins centralisée des responsabilités, il convient d'observer que l'authentification, visant l'accès à des prestations électroniques de services gouvernementaux, ne requiert pas systématiquement la mise en œuvre d'une identité numérique gouvernementale.

Le modèle français, avec l'introduction en 2016 de FranceConnect[12], constitue une illustration parfaite de cette approche. À l'origine, FranceConnect est apparu comme une solution destinée à faciliter l'accès aux multiples services en ligne du

[12] https://franceconnect.gouv.fr

gouvernement, en se positionnant comme un fédérateur d'identités. Concrètement, l'utilisateur choisit parmi plusieurs fournisseurs d'identités autorisés – par exemple, impots.gouv.fr, ameli.fr ou La Poste – pour se connecter à d'autres plateformes publiques affiliées, sans devoir créer de nouveaux comptes ni mémoriser différents identifiants.

L'objectif initial était donc de simplifier l'expérience citoyenne tout en garantissant un niveau de protection conforme aux obligations légales françaises en matière de confidentialité et de sécurité.

Le projet d'identité numérique étatique qui porte le nom de « France Identité » a été déployé à échelle réelle bien plus tard, en 2023, et se présente comme un nouveau fournisseur d'identité, qui s'ajoute aux précédents, avec la spécificité d'atteindre un niveau de sécurité supérieur[13].

Recommandation 5 : Établir un cadre de gouvernance clair et sécuritaire et s'ouvrir à plusieurs fournisseurs d'identité – idéalement des organismes publics – supprimant, ainsi, le besoin d'un registre d'identification unique pour l'identité numérique nationale.

Lors des auditions et consultations particulières du projet de loi 95, modifiant la loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI), plusieurs experts, dont notamment les professeurs Sébastien Gambs et Benoît Dupont, avaient attiré l'attention sur les risques d'une centralisation des données et sur l'opportunité de recourir à des architectures qui favorisent une gestion moins centralisée de la donnée.

Dans ce contexte, le ministre Éric Caire avait déclaré, *« dans le fond, 95 ne change pas qui peut avoir accès à quoi. 95 change comment j'accède à la donnée »*[14].

L'objectif clairement défendu était donc de créer un cadre juridique qui permettrait la circulation des données entre les dépositaires de données numériques gouvernementales et les autres organismes publics, à des fins administratives et de service public.

Au reste, il semble que l'instauration d'un registre numérique de l'identité numérique nationale pourrait conduire dans un sens différent. Suivant la définition qui en est donnée dans le projet de loi, ce registre est un système de dépôt et de communication de données qui doit permettre notamment la conservation sécuritaire, pour le compte d'un organisme public, de tout ou partie de ces données ; la communication entre organismes publics de ces données ; l'accès à ces données ; la traçabilité de tout accès au registre par une personne, que ce soit pour y déposer ces données, les

[13] https://franceconnect.gouv.fr/france-identite

[14] *Journal des débats de la Commission des finances publiques – Assemblée nationale du Québec*, Québec, 2021.

utiliser ou en recevoir la communication et toute autre fonctionnalité déterminée par règlement du ministre.

Ce système peut apparaître comme une sorte de coffre-fort, qui permettrait une gestion particulièrement rigoureuse de la sécurité des données numériques gouvernementales. Cette approche conduit à créer un point de défaillance unique qui peut avoir des conséquences dramatiques sur la vie des citoyens. Conforme à l'objectif initialement défendu par le ministre Caire, une approche décentralisée des sources de données gouvernementales et de la prestation électronique de service gouvernementale serait plus sécuritaire et pourrait offrir des gains d'efficience.

Ce modèle qu'on retrouve, par exemple en Estonie, repose sur une architecture qui distingue entre les sources de données et l'infrastructure de communication et d'utilisation des données[15]. Ainsi, chaque organisme public conserve les responsabilités afférentes au traitement des données qu'il collecte et est tenu de respecter les différents standards gouvernementaux.

Ce système évite la centralisation des informations dans un registre ou un dépôt unique, tout en assurant une interopérabilité efficace entre les différentes entités administratives. Cette interopérabilité est rendue possible par une infrastructure technique appelée X-Road, qui agit comme une couche intermédiaire sécurisée facilitant les échanges de données entre les systèmes. Cette couche standardise les communications entre les bases de données et garantit que celles-ci se déroulent de manière sécurisée et traçable. Les données ne sont pas copiées ou centralisées, chaque organisme reste le seul dépositaire des informations qu'il collecte, renforçant ainsi la souveraineté des données et limitant les risques liés à la centralisation.

La sécurité et la transparence de ces échanges reposent sur deux éléments fondamentaux : les systèmes d'horodatage et les mécanismes de gestion des journaux (logs). Chaque transaction impliquant des données personnelles ou administratives est horodatée de manière précise, enregistrant ainsi la date et l'heure exactes de l'opération. Cela permet de reconstruire intégralement le cheminement des données en cas d'audit ou d'enquête. Par ailleurs, chaque interaction avec le système est consignée dans des journaux immuables, incluant l'identité de l'utilisateur ou de l'entité ayant accédé aux données, la nature de l'opération effectuée, ainsi que la finalité de l'accès. Ces logs garantissent une traçabilité complète et sont soumis à des mécanismes de supervision indépendants. En Estonie, cette transparence se traduit également par la possibilité pour chaque citoyen de consulter l'historique des accès à ses données personnelles, ce qui renforce la confiance du public dans l'infrastructure numérique.

Ce modèle décentralisé présente de nombreux avantages. Il élimine le risque d'un point de défaillance unique, caractéristique des systèmes centralisés, et limite ainsi les conséquences d'une cyberattaque ou d'une panne sur l'ensemble du réseau. Il améliore également la sécurité des données grâce à l'utilisation systématique du cryptage, de l'horodatage et des logs, tout en garantissant une protection accrue de

[15] *Estonia: A Successfully Integrated Population-Registration and ID Management System | Get Every One in the Picture*, par World Bank Group, 2015.

la vie privée des citoyens. La modularité de l'architecture offre une flexibilité et une évolutivité remarquables, permettant d'ajouter de nouveaux services ou de connecter des bases de données supplémentaires sans compromettre la structure existante. Enfin, ce système garantit un usage conforme aux principes de minimisation des données, limitant ainsi les abus potentiels liés à l'accès ou à la manipulation des informations personnelles.

Dans le contexte québécois, une architecture inspirée du modèle estonien pour le registre numérique de l'identité nationale serait particulièrement pertinente. Elle permettrait de respecter les objectifs initiaux de la LGGRI, notamment en assurant une communication fluide et sécurisée entre les différents organismes publics, tout en évitant les écueils d'une centralisation excessive. Ce modèle offrirait une solution résiliente et fiable pour la gestion des données numériques, tout en renforçant la confiance des citoyens dans les services numériques gouvernementaux. L'approche modulaire garantirait une gestion rigoureuse de la sécurité et de la traçabilité des données, limitant les risques d'abus ou de failles systémiques, et répondrait pleinement aux exigences de transparence, d'efficacité et de protection des droits des citoyens dans un cadre numérique moderne.

Recommandation 6 : Opter pour un modèle de l'identité numérique nationale et de la prestation de service électronique gouvernementale intégrée, fondé sur l'interopérabilité.

Recommandation 7 : Modifier le projet de loi en conséquence.

Recommandation 8 : Instaurer une infrastructure nationale d'échange de données numériques gouvernementales à la place du registre national de l'identité numérique.

5. CONCLUSION

Le projet de loi 82 marque un moment charnière dans l'histoire numérique du Québec, en particulier dans la manière dont l'État envisage la gestion de l'identité numérique de ses citoyens. Il constitue une opportunité historique de redonner le pouvoir au citoyen sur son identité dans l'univers numérique, marqué aujourd'hui par des dynamiques du marché qui relèguent parfois au second plan la centralité de l'individu et considèrent la donnée uniquement comme un objet monétisable. Pour saisir pleinement cette opportunité, il est essentiel que le PL ne considère pas uniquement la donnée sous son aspect utilitaire, mais qu'il l'apprécie dans son rapport avec le citoyen, sous l'angle de la reconnaissance juridique de ce dernier. Clairement, il s'agit de renforcer la souveraineté individuelle dans un monde interconnecté, tout en affirmant les valeurs démocratiques fondamentales du Québec.

La mise en œuvre d'un projet aussi ambitieux ne peut se faire en vase clos. Elle nécessite une collaboration étroite entre toutes les parties prenantes. Sur le plan institutionnel, une coordination avec les autres provinces canadiennes et le gouvernement fédéral est essentielle pour assurer l'interopérabilité et la reconnaissance mutuelle des identités numériques à travers le pays. En ce sens, l'implication du Québec dans la réalisation du cadre de confiance pancanadien est à féliciter. Il est essentiel, que ce soit à travers cette tribune ou une autre, que la collaboration intergouvernementale s'effectue suivant une vision commune, centrée sur le citoyen.

Au-delà des collaborations institutionnelles, ce projet doit également mobiliser toutes les forces vives de la société québécoise. Les citoyens, les organisations de la société civile, les experts en technologie, les juristes et les chercheurs doivent être impliqués activement dans le processus. Le Québec bénéficie d'une expertise de premier plan en matière de gouvernance numérique, d'identité numérique auto-souveraine et de technologies décentralisées, comme en témoignent les travaux des organisations et des chaires de recherche actives dans ces domaines. Ces ressources peuvent jouer un rôle stratégique en accompagnant le gouvernement dans ses efforts de conception, de mise en œuvre et de gestion d'une identité numérique nationale.

Le projet de loi 82 ne doit pas seulement être une réforme technique visant à moderniser les infrastructures numériques du Québec ; il doit poser les bases d'un cadre durable, transparent et inclusif qui renforcera la confiance des citoyens dans l'État et ses institutions. En s'appuyant sur les principes d'autonomie, de collaboration et de transparence, le gouvernement a l'occasion de poser les bases d'un système d'identité numérique qui non seulement répondra aux exigences de l'ère numérique, mais placera également le citoyen au cœur de cette révolution.

Pour toutes questions, communiquez avec :

M. Jean-François Gauthier
Président-directeur général
Institut de gouvernance numérique
Courriel : JFGauthier@IGN.quebec
Cellulaire : 418 558-0586