Commission d'accès à l'information du Québec

CFP - 016M
C. P. PL 82
Loi concernant l'identité numérique

Projet de loi nº 82, *Loi concernant l'identité numérique et modifiant d'autres dispositions*

Mémoire de la Commission d'accès à l'information présenté à la Commission des finances publiques dans le cadre des consultations particulières et auditions publiques

Québec, le 27 janvier 2025

Table des matières

1. Introduction

À titre d'organisme qui veille au respect et à la promotion des droits des citoyens quant à la protection de leurs renseignements personnels, la Commission d'accès à l'information (ci-après, la Commission) soumet le présent mémoire concernant le projet de loi nº 82 intitulé Loi concernant l'identité numérique nationale et modifiant d'autres dispositions (ci-après, le projet de loi), lequel a été présenté lors de la séance du 21 novembre 2024 à l'Assemblée nationale du Québec.

Ce projet de loi apporte des modifications notamment à la *Loi sur l'administration fiscale*[1], à la *Loi sur l'assurance maladie*[2], à la *Loi concernant le cadre juridique des technologies de l'information*[3], à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*[4], à la *Loi sur le ministère de l'Emploi et de la Solidarité sociale et sur la Commission des partenaires du marché du travail*[5] ainsi qu'à la *Loi sur le ministère de la Cybersécurité et du Numérique*[6]. Ce projet de loi modifie également trois règlements[7].

Les développements relatifs à l'identité numérique (ci-après, l'IN) sont au cœur de l'évolution des systèmes numériques qui permettent des communications, des échanges ainsi que des transactions sécurisés, efficaces et fiables entre les citoyens, les entreprises et les différentes branches de l'appareil étatique. Ces développements s'inscrivent dans une tendance mondiale en la matière dont les balbutiements ont commencé à la fin des années 90 et au début des années 2000[8] et qui se poursuivent aujourd'hui. En effet, dans les dernières années, plusieurs États ont mis en place l'équivalent d'une IN nationale[9] tandis que le Québec et d'autres provinces canadiennes souhaitent en introduire une dans les prochaines années. Or, l'IN nationale est susceptible d'avoir un impact significatif dans la sphère des services numériques publics et privés.

En effet, les avantages d'une IN robuste, bien élaborée et largement adoptée par les citoyens peuvent être nombreux : la simplification des transactions sécurisées entre les citoyens, les entreprises et l'État, une réduction de la circulation et de la divulgation des renseignements personnels des citoyens, une protection accrue contre la fraude et le vol d'identité, une

[1] RLRQ, c. A-6.002, ci-après, la LAF.
[2] RLRQ, c. A-29, ci-après, la LAM.
[3] RLRQ, c. C-1.1, ci-après, la LCCJTI.
[4] RLRQ, c. G-1.03, ci-après, la LGGRI.
[5] RLRQ, c. M-15.001, ci-après, la LMESS.
[6] RLRQ, c. M-17.1.1, ci-après, la LMCN.
[7] *Règlement sur la publicité foncière*, RLRQ, c. CCQ, r. 6; *Règlement sur les contrats des organismes publics en matière de technologies de l'information*, RLRQ, c. C-65.1, r. 5.1; et *Règlement sur les contrats du gouvernement pour la location d'immeubles*, RLRQ, c. C-65.1, r. 7.
[8] Félix GARIÉPY et Benoit DUPONT, *Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale*, 2023, p. 6-8, en ligne : <https://www.obvia.ca/sites/obvia.ca/files/ressources/Guide%20sur%20les%20conditions%20et%20bonnes%20pratiques%20pour%20la%20mise%20en%20place%20d%27une%20identit%C3%A9%20num%C3%A9rique%20nationale.pdf>, p. 15 et suiv.
[9] *Ibid*.

amélioration de l'accessibilité du citoyen à ses renseignements et à certains services, etc. En somme, une IN nationale adéquatement conçue et mise en application offre au citoyen un meilleur contrôle sur ses renseignements personnels.

En revanche, des conséquences négatives importantes, de nombreux inconvénients et des risques significatifs peuvent suivre la mise en place d'une IN nationale si les précautions nécessaires ne sont pas prises, si les assises juridiques et en matière de gouvernance sont insuffisantes. Un tel contexte pourrait mener vers une réduction de la protection des renseignements personnels des citoyens. De nombreux enjeux peuvent alors se présenter, notamment :

- Sans encadrement adéquat, l'IN nationale peut entraîner la collecte massive de renseignements sur les citoyens et ainsi alimenter le profilage et même mener à la surveillance de ceux-ci;
- Si les processus mis en place ne prévoient pas le consentement exprès des citoyens pour toute communication ou utilisation des attestations gouvernementales ou des éléments relatifs à l'IN nationale, le citoyen peut perdre le contrôle sur ses renseignements;
- Si les processus mis en place ne sont pas suffisamment robustes et sécuritaires, les risques relatifs à la protection des renseignements personnels augmentent;
- L'insuffisance de l'encadrement juridique peut également engendrer une diminution de la protection de la vie privée des citoyens ainsi qu'une perte de confiance des différents acteurs liés à l'utilisation de l'IN nationale[10];
- Si l'encadrement juridique n'est pas suffisamment étoffé, il devient difficile de comprendre le système d'IN mis en place;
- Finalement, l'accumulation de ces enjeux peut fortement influencer l'adhésion des citoyens à cette IN nationale.

La Commission salue l'initiative gouvernementale d'enchâsser législativement l'encadrement relatif à l'IN nationale et souhaite que cette initiative conduise à l'adoption d'un projet de loi qui mettra en place toutes les assises nécessaires à l'IN nationale. Au surplus, la Commission est d'avis qu'une IN nationale adéquatement encadrée, robuste et sécuritaire favorise la protection des renseignements personnels des citoyens. Cependant, la Commission insiste sur le fait que cet encadrement doit être suffisamment exhaustif et précis pour éviter les dérives vers lesquelles une telle initiative peut mener[11], mais surtout, pour assurer une importante adhésion à cette IN nationale. C'est pourquoi, de l'avis de la Commission, l'encadrement juridique relatif à l'IN nationale doit, au minimum, contenir des dispositions visant à[12] :

[10] Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale, précité note 8, p. 12.
[11] *Ibid*., concernant l'expérience de l'Inde dans la mise en place d'une identité numérique nationale.
[12] À ce sujet, voir la résolution des commissaires à la protection de la vie privée fédéral, provinciaux et territoriaux et des ombudsmans du Canada, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-

- Limiter toute utilisation secondaire des renseignements pour le ministre et notamment, interdire fermement à toute organisation publique ou privée l'utilisation des renseignements générés par l'utilisation de l'IN nationale ou de toute attestation émise par une organisation publique ou privée relatifs à cette identité à des fins de surveillance de la population, de traçage et de profilage;
- Assurer que la participation des citoyens est libre, volontaire et facultative. Les systèmes relatifs à l'IN doivent offrir des options ou des alternatives aux citoyens qui ne souhaitent pas l'utiliser;
- Assurer le plein contrôle des citoyens de leurs renseignements personnels et, notamment, voir à ce que seuls les renseignements personnels nécessaires soient recueillis, utilisés, communiqués ou conservés;
- Prévoir que chaque utilisation ou communication de renseignements des citoyens fasse l'objet d'un consentement exprès et éclairé de la part de ceux-ci;
- Limiter la collecte ou l'utilisation de renseignements sensibles, comme les renseignements biométriques, aux seuls cas où d'autres moyens moins intrusifs ne permettent pas d'atteindre l'objectif poursuivi;
- Assurer la mise en place d'un modèle ainsi que des mesures de sécurité suffisantes;
- Assurer que les processus mis en place sont transparents, que les objectifs des systèmes d'IN soient diffusés, que les renseignements personnels utilisés ainsi que la manière dont ils sont utilisés et les personnes qui sont susceptibles de les utiliser soient connus;
- Prévoir des sanctions à toute violation de l'encadrement juridique mis en place ainsi que des recours pour les citoyens;
- Prévoir l'existence d'une autorité indépendante qui surveille l'application des dispositions de la loi relatives à l'IN nationale.

De l'avis de la Commission, l'encadrement juridique existant ainsi que le projet de loi couvrent une partie des éléments mentionnés ci-dessus. En revanche, de nombreux principes et dispositions essentiels sont manquants et devraient, selon la Commission, être ajoutés au projet de loi.

Dans son mémoire, la Commission souhaite expliquer plus en détail l'IN avant d'aborder son analyse détaillée des dispositions du projet de loi. La Commission commentera également certaines des modifications apportées à d'autres lois par le projet de loi, plus particulièrement les modifications proposées à la LAM, à la LGGRI et à la LAF.

territoires/res_220921_02/> et les commentaires de la Commission concernant cette résolution, en ligne : <https://www.cai.gouv.qc.ca/actualites/identite-numerique-canada-organismes-surveillance-demandent-gouvernements-assurer-droit-vie-privee-et-transparence-dans-projets-et-systemes?gt=identit%C3%A9%20num%C3%A9rique>.

2. Le projet de loi nº 82 – L'identité numérique nationale

Pour comprendre adéquatement l'analyse du projet de loi effectuée par la Commission, il est indispensable de comprendre ce qu'est l'IN et qui sont les principaux acteurs impliqués dans un écosystème d'IN.

De plus, pour comprendre la nécessité d'apporter certaines modifications au projet de loi, la Commission souhaite également expliquer les principaux avantages de l'IN, les principaux risques auxquels s'exposent la société québécoise sans assises juridiques solides en matière d'IN ainsi que les balises à implanter dans tout projet d'IN pour assurer la protection des renseignements personnels.

Finalement, avant d'aborder l'analyse du projet de loi, la Commission souhaite présenter aux parlementaires quelques initiatives d'autres juridictions en matière d'IN.

2.1. L'identité numérique

2.1.1. L'identité numérique, qu'est-ce que c'est?

L'IN est une notion complexe et en mouvance, si bien qu'il est ardu d'en arrêter une définition précise. Celle-ci change en effet en fonction du champ d'études par lequel on l'aborde, et peut même connaître plusieurs variations au sein d'une même discipline[13]. Elle ne fait pas l'objet d'un consensus juridique ou scientifique quant à sa nature ou à son extension exacte. Considérant ce flou persistant, l'IN est généralement comprise par référence à ses différents éléments constitutifs ainsi que par les fonctions et usages qu'on lui réserve. Ainsi, l'IN correspond à un ensemble d'attributs, regroupés en format numérique, permettant à une personne, soit-elle physique ou morale, d'interagir de façon sécuritaire avec d'autres entités, que ce soit afin de s'identifier et de s'authentifier, ou encore afin de produire la preuve de la possession de certains

[13] Voir GROUPE DE RECHERCHE INTERDISCIPLINAIRE EN CYBERSÉCURITÉ, *Guide d'encadrement sécuritaire de l'identité numérique*, Université de Sherbrooke, 2022, p. 8, en ligne : <https://gric.recherche.usherbrooke.ca/wp-content/uploads/2022/04/GUIDE_ENCADREMENT_SECURITAIRE_IDENTITE_NUMERIQUE.pdf>; CONSEIL NATIONAL DU NUMÉRIQUE, *Identités numériques. Clés de voûte de la citoyenneté numérique*, Conseil national du numérique, 2020, p. 25, en ligne : <https://cnnumerique.fr/files/uploads/2020/2020.06.19.ra-cnnum-idnum-web3.pdf>.

attributs[14][15]. Un bref examen de ces éléments permettra de démystifier l'IN et de poser les premiers jalons d'une compréhension basique de ce phénomène.

Avant toute chose, il doit être noté que l'identité ne se limite pas au seul état civil d'une personne. Bien au contraire, chacun assume au quotidien différentes identités en fonction du contexte où il est plongé[16]. Nous avons par exemple une identité professionnelle contrastant avec celles que l'on assume dans notre vie privée, et d'autres encore sur les réseaux sociaux ou sur différentes plateformes. Ces différentes identités ne se basent pas toutes sur les caractéristiques reliées à l'identité civile; certaines peuvent par exemple s'appuyer sur des pseudonymes, comme c'est fréquemment le cas dans le quotidien numérique. Ces différentes identités d'un même individu peuvent être reflétées dans l'IN, et lui permettre d'interagir avec une gamme variée d'organisations, tant des sphères de l'administration publique et du privé.

Ces identités prennent elles aussi forme par l'agrégation de différents attributs constitutifs. Le terme « attribut » désigne ici une « particularité, qualité ou caractéristique vérifiée qui a été attribuée à un utilisateur[17] ». Comme le laisse percevoir la généralité de cette définition, il existe une foule diverse et variée d'attributs pouvant être reliés à une identité, certains stables, d'autres changeants. Dans une vaste proportion, il s'agira de renseignements personnels, soit de renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier[18]. C'est par exemple le cas des renseignements reliés à l'identité civile de la personne, tels le nom et l'adresse de résidence, de ses renseignements biométriques, comme ses empreintes digitales ou le produit de la reconnaissance faciale, ou encore des données associées à sa géolocalisation. Dans le cadre de l'IN, les attributs possédés par une personne sont vérifiés, c'est-à-dire qu'une entité de confiance assure leur authenticité, ainsi que le lien qui les relie à une identité donnée. Les attributs peuvent alors être employés à l'identification ou l'authentification d'une identité par un fournisseur de service que l'on désignera comme consommateur ou vérificateur de l'IN, ou encore être vérifiés eux-mêmes. Ce sera par exemple le cas pour un fournisseur de service voulant s'assurer de faire affaire à une personne majeure. Diverses attestations peuvent également être intégrées parmi les attributs associés à une identité.

L'IN se déploie par l'entremise de différents supports et structures. En guise d'exemple, tel que mentionné ci-haut, les attributs possédés par une personne peuvent se matérialiser au moyen d'attestations distinctes et vérifiables, lesquelles peuvent être présentées à la pièce aux différents fournisseurs de services. Celles-ci peuvent être regroupées au sein d'un « portefeuille

---

[14] Voir notamment BENEVA, DESJARDINS, KPMG, TELUS, VIDÉOTRON, et LABORATOIRE D'IDENTITÉ NUMÉRIQUE, *Vivre à l'ère numérique en toute confiance, c'est possible*, 2023, en ligne : <https://www.idlab.org/wp-content/uploads/2023/05/Vf_Livre_Blanc_IN_V6.3.pdf>; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Dossier thématique - L'identité numérique*, 2023, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_dossier-thematique_identite-numerique.pdf>; GROUPE DE RECHERCHE INTERDISCIPLINAIRE EN CYBERSÉCURITÉ, précité, note 13; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, « Recommandation du Conseil sur la gouvernance de l'identité numérique » (juin 2023), en ligne : <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0491> (consulté le 20 janvier 2025); CONSEIL NATIONAL DU numérique, précité, note 13.

[15] Si l'identité numérique peut effectivement concerner des personnes ou des organisations, voire des objets, le présent mémoire se concentrera sur les personnes.

[16] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 14, p. 2.

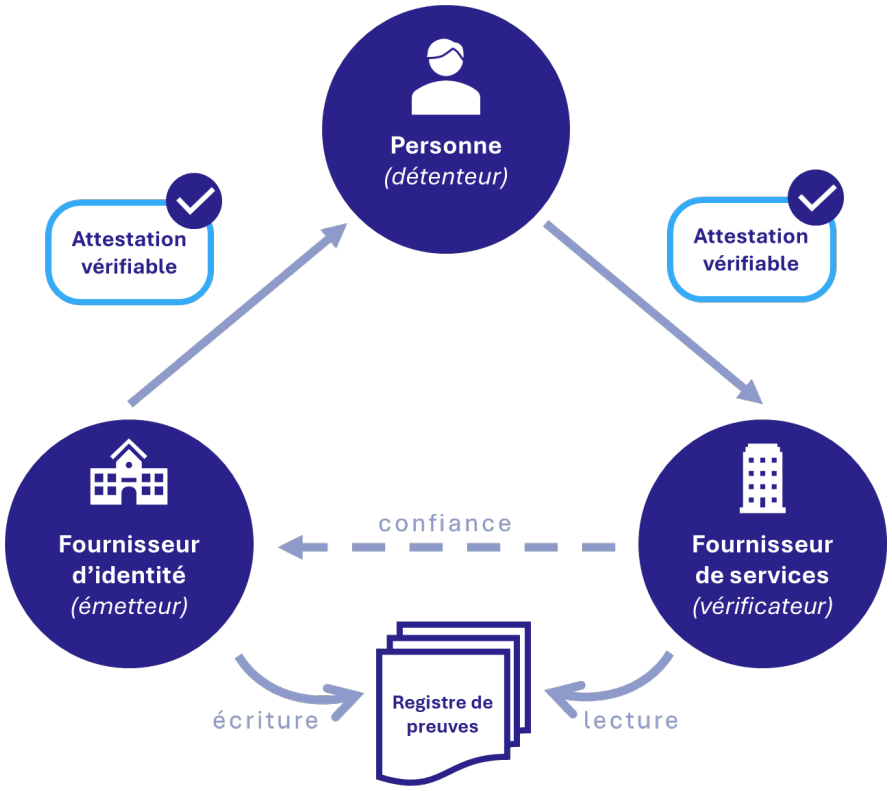
[17] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 14.

[18] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, article 54, ci-après, la Loi sur l'accès.

numérique » faisant office de dépôt sécurisé à la disposition de la personne concernée. Au-delà de ces composantes, l'IN peut être déployé via divers supports, qu'il s'agisse de cartes à puce, de sites Web ou encore d'applications pour appareils mobiles.

Si l'IN est une notion complexe, le besoin auquel elle doit répondre est simple et bien connu. Il s'agit de pouvoir s'identifier et s'authentifier efficacement auprès des fournisseurs de services. Ce sont là des processus courants dans la vie quotidienne, à la fois dans et hors la sphère du numérique. L'identification permet de s'afficher comme personne distincte, et l'authentification consiste à prouver la véracité de cette identité. Dans les faits, saisir un nom de compte et un mot de passe pour accéder à une plateforme en ligne représente une manifestation de ce processus, ainsi qu'une forme d'IN. L'IN permet de surcroît à la personne d'apporter la preuve qu'elle possède les attributs nécessaires à la fourniture d'un service donné.

Cette démarche d'identification et d'authentification repose sur l'interaction d'au moins trois acteurs, qu'elle soit accomplie ou non au moyen de l'IN. C'est ce que l'on qualifie de « triangle de la confiance[19] » : la personne souhaitant accéder à un service donné, que ce soit en ligne ou hors ligne, doit fournir des preuves de son identité au fournisseur de services. Elle y arrive par la production d'attestations émises par un tiers de confiance, le fournisseur d'identité, auprès duquel le fournisseur de service peut vérifier l'authenticité des attestations, notamment via la consultation d'un registre de preuves.



[19] BENEVA et al., précité, note 14, p. 7; Commission nationale de l'informatique et des libertés, précité, note 14, p. 4; F. Gariépy et B. Dupont, précité, note 8, p. 6-8, en ligne : <https://www.obvia.ca/sites/obvia.ca/files/ressources/Guide%20sur%20les%20conditions%20et%20bonnes%20pratiques%20pour%20la%20mise%20en%20place%20d%27une%20identit%C3%A9%20num%C3%A9rique%20nationale.pdf>.

Ces trois acteurs peuvent interagir au sein de modèles d'IN plus ou moins élaborés[20]. Le modèle isolé, relevant de la première génération de l'IN, met en relation la personne avec un fournisseur de service agissant aussi comme fournisseur d'identité. C'est par exemple le cas pour les différents comptes qu'une personne peut ouvrir sur diverses plateformes, et qui ne fonctionnent qu'auprès de celles-ci. C'est de ce modèle peu pratique que les projets d'IN modernes cherchent à s'éloigner. En effet, ce modèle non interopérable suppose pour l'utilisateur un grand nombre de combinaison d'identifiants et de mots de passe. De plus, puisque toutes les informations sont en possession des différentes organisations où une IN est créée, la surface d'attaque pour des acteurs malveillants est accrue.

Le modèle fédéré, quant à lui, permet à la personne d'entrer en relation avec plusieurs fournisseurs de services en s'en remettant à un seul fournisseur d'identité. Un modèle où seule l'administration publique fournissait des attestations en serait un exemple. Comparativement au modèle isolé, celui-ci facilite l'authentification pour l'utilisateur et permet une certaine interopérabilité. On note cependant que comme tous les renseignements reposent entre les mains d'un même fournisseur d'identité, ceci augmente les risques lors d'un incident de confidentialité. Dans les faits, un incident de confidentialité auprès du fournisseur d'identité peut avoir un impact sur l'ensemble des acteurs et exposer chacun des liens qu'entretiennent les détenteurs avec les fournisseurs de services dans l'écosystème touché.

Enfin, le modèle décentralisé place la personne au centre du processus. En effet, il lui laisse le choix de différents fournisseurs d'identités dans ses relations avec les divers fournisseurs de services.

Cette esquisse du fonctionnement de l'IN et de sa matérialisation montre qu'elle se déploie nécessairement au sein d'un écosystème composé de plusieurs acteurs pouvant relever tant du public que du privé, soumis à un ensemble de processus, de politiques et de règles partagées[21]. L'implantation efficace d'un modèle ambitieux d'IN dépend de la clarté et de la solidité des processus et de son cadre de gouvernance. En effet, l'adoption de l'IN est directement tributaire du degré de confiance que la population sera prête à lui accorder. Afin que celle-ci franchisse le pas, il sera par conséquent nécessaire de lui donner les moyens de comprendre le cadre au sein duquel on l'invite à s'insérer et de lui donner des garanties de sécurité et de contrôle.

Par surcroît, considérant la nature des renseignements personnels impliqués dans un projet d'IN national et les fournisseurs de services potentiels de son écosystème, il est nécessaire de sensibiliser la population non seulement à ses avantages, mais aussi à ses risques et, plus largement, à l'importance névralgique qu'elle pourrait avoir dans le quotidien de chacun. Comme l'IN est une affaire d'échange de renseignements personnels parfois sensibles par nature ou par contexte entre différents acteurs, son déploiement doit être fait dans les règles de l'art, sans quoi les personnes peuvent être exposées à d'importants préjudices.

---

[20] F. GARIÉPY et B. DUPONT, précité, note 8, p. 6-8.

[21] COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX ET DES OMBUDSMANS QUI ASSUMENT UNE FONCTION DE SURVEILLANCE DANS LE DOMAINE, « Assurer le droit à la vie privée et la transparence dans l'écosystème d'identité numérique au Canada », *Commissariat à la protection de la vie privée du Canada* (21 septembre 2022), en ligne : <https://priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_220921_02/> (consulté le 24 octobre 2022); F. GARIÉPY et B. DUPONT, précité, note 8, p. 5, voir note 13. ; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 14.

2.1.2. Les avantages attendus de l'identité numérique en matière de protection des renseignements personnels

Dans le contexte d'aujourd'hui, marqué par le tournant numérique, l'IN est la nouvelle pierre angulaire des relations entre les personnes et les organisations publiques et privées. Dans la mesure où il est implanté dans le respect des meilleures pratiques, un modèle d'IN promet des interactions plus efficaces et commodes avec les organisations, un meilleur contrôle des individus sur leurs renseignements personnels ainsi qu'une minimisation de leur circulation. Le numérique entraîne cependant dans son sillage de nouvelles menaces, notamment en matière de sécurité de l'information. Une solution d'IN véritablement efficace doit aussi pallier cette nouvelle réalité en offrant des protections accrues contre la fraude et les cyberattaques.

L'IN promet de faciliter les relations entre les personnes et les différents fournisseurs de services avec lesquels elles font affaire. Tel que mentionné à la section précédente, un modèle fédéré ou décentralisé rend possible une meilleure gestion des identifiants et des authentifiants : les personnes n'ont plus à créer une multiplicité de comptes afin d'interagir avec les fournisseurs. L'interopérabilité est alors synonyme de gains en temps et en efficacité au quotidien. L'IN comprend toutes les commodités associées au numérique : elle facilite l'accès à une gamme diverse de services, et ce, même en cas de contrainte empêchant les déplacements, elle diminue les temps d'attente et les efforts à déployer et elle permet de corriger rapidement les erreurs ou de s'assurer de l'exactitude des renseignements fournis. Elle permet aussi aux organisations d'accroître leur degré de certitude quant à la véracité de l'identité déclarée et des attributs de leurs clients et de les intégrer à leurs services avec moins de friction, notamment au niveau administratif.

Au-delà de ces avantages non négligeables sur le déroulement des interactions entre les personnes et les organisations, l'IN bien déployée permet d'assurer aux personnes une divulgation moindre de leurs renseignements personnels ainsi qu'un meilleur contrôle sur ceux-ci. Par l'entremise du système d'attestations, il est en effet possible de limiter le nombre de renseignements personnels divulgués afin de s'identifier ou de prouver un attribut. Par exemple, une personne n'aura plus à fournir des pièces d'identité comprenant plusieurs renseignements personnels, comme un permis de conduire (photo, numéro unique, adresse, condition ayant une incidence sur la conduite, taille, couleur des yeux, etc.), afin de prouver à une organisation qu'elle a 18 ans ou plus; elle pourra se contenter de divulguer un seul attribut attestant de sa majorité. D'ailleurs, l'IN permet la mise en place de techniques cryptographiques favorisant la protection des renseignements personnels, telle la preuve à divulgation nulle de connaissance[22], qui permet à une partie d'authentifier un attribut sans que le renseignement personnel ne soit transmis à la partie qui demande confirmation. Pour reprendre l'exemple de l'âge, il devient possible de confirmer que la personne est majeure sans même collecter sa date de naissance.

La divulgation sélective des attributs et la preuve à divulgation nulle de connaissance relèvent toutes deux de la minimisation de la collecte, un principe fondamental en matière de protection des renseignements personnels. La minimisation est, en toute logique, la première et la meilleure

[22] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 14, p. 11; COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX ET DES OMBUDSMANS QUI ASSUMENT UNE FONCTION DE SURVEILLANCE DANS LE DOMAINE, précité, note 21.

garantie que des renseignements personnels ne soient pas utilisés de façon inadéquate ou malveillante : on ne peut abuser de renseignements dont on ne dispose pas.

Similairement, un modèle d'IN centré sur l'individu lui donne le plein contrôle de ses renseignements personnels. Il revient à la personne de choisir précisément quels attributs elle souhaite partager à l'organisation avec laquelle elle interagit. En contrôle de ses attestations, elle peut exercer librement et aisément son consentement au traitement de ses renseignements et le retirer tout aussi simplement. Le consentement est ainsi un autre socle majeur des lois en matière de protection des renseignements personnels qu'un système d'IN doit contribuer à renforcer.

Par surcroît, l'IN, à l'instar d'autres systèmes numériques, suppose que subsistent des traces des utilisations des attributs fournis par les personnes aux organisations. Cette journalisation des traitements de renseignements peut aider les personnes à exercer leur contrôle et leurs droits en leur permettant de vérifier à tout moment quelles organisations ont consulté ou utilisé leurs attributs.

Enfin, l'IN doit permettre un rehaussement de la sécurité des renseignements personnels. Un modèle d'IN adéquatement développé réduit les risques de vol d'identité et de fraude. À cette fin, plusieurs mesures sont possibles en supplément des processus d'authentification et de chiffrement des attributs. À titre d'exemple, un modèle décentralisé, au sein duquel les attributs ne sont pas conservés dans une banque de données aux mains d'un seul fournisseur d'identité, réduit considérablement la surface d'attaque d'acteurs malicieux[23]. En cas de fraude ou de vol d'identité avéré, des mesures pourraient permettre à la personne concernée la désactivation de son IN[24]. Cette révocabilité est une amélioration importante relativement à la situation actuelle, où il arrive que des renseignements personnels au cœur de la relation des citoyens avec l'État, tel le numéro d'assurance sociale, circulent et sont utilisés par des acteurs malveillants sans que les personnes puissent exercer de recours.

En bout de ligne, l'IN, en plus de rendre les interactions plus commodes et les services plus accessibles, doit permettre l'atteinte d'un niveau de sécurité accru à l'échelle sociétale. Ce rehaussement passe notamment par l'établissement de différentes mesures de sécurité, par un plus grand contrôle des individus sur leurs renseignements personnels ainsi que par la circulation et la conservation moindre de ceux-ci.

2.1.3. Les risques relatifs à l'identité numérique en matière de protection des renseignements personnels

Les risques associés à l'IN touchent aux mêmes points que ses avantages potentiels. En effet, un système dont l'implantation serait défaillante, que ce soit au niveau de son architecture, de ses choix de conception, des technologies employées ou de la gouvernance, peut avoir un impact négatif sur les droits et les libertés des personnes, et ce, particulièrement eu égard à la protection de leur vie privée, en plus d'exposer davantage les personnes à la fraude et au vol d'identité.

[23] BENEVA et al., précité, note 14, p. 22.
[24] *Id.*, p. 21.

Les IN sont susceptibles de contenir de nombreux renseignements personnels, dont certains sont particulièrement sensibles par nature ou par contexte. Cela est particulièrement vrai pour les systèmes d'IN nationaux, qui incluent divers renseignements concernant l'identité des personnes et leurs relations avec l'administration publique. Certains autres renseignements particulièrement sensibles peuvent y être joints en fonction des caractéristiques du modèle retenu. Par exemple, un système peut comprendre des renseignements biométriques, comme les empreintes digitales ou la reconnaissance faciale, à des fins d'authentification des personnes[25].

Les interactions numériques laissent forcément de nombreuses traces. Pour les personnes, cela signifie qu'une importante somme de renseignements personnels peut s'ajouter à leur IN au fur et à mesure qu'elles en font usage. Il peut s'agir autant de traces directes qu'elles laissent, par exemple des commentaires sur une page, que des métadonnées, soit des renseignements à propos de leurs interactions[26]. L'historique de navigation sur une page ou l'historique d'achat, l'adresse IP de l'appareil utilisé, la géolocalisation, la date et l'heure de consultation en sont autant d'exemples. Au surplus, des renseignements personnels supplémentaires peuvent être inférés par l'analyse algorithmique des renseignements rattachés à l'IN d'une personne, qu'il s'agisse des renseignements rattachés à son identité ou de ceux produits par son utilisation du système. Parmi les renseignements que l'on peut inférer sur une personne, nombreux peuvent être de nature sensible, que ce soit par leur nature ou par contexte. Il peut par exemple s'agir de renseignements portant sur le sentiment religieux, les opinions politiques, l'orientation sexuelle ou encore sur l'état de santé physique ou mentale de la personne.

Le numérique, et l'IN n'y échappe pas, ouvre ainsi la possibilité au traçage et à un profilage extrêmement détaillé et invasif de la vie privée des personnes. Cette possibilité, en soi nuisible si la personne n'y consent pas, peut s'avérer particulièrement problématique s'il est employé à des fins de discrimination ou de manipulation. À ce titre, il importe qu'un système d'IN ne soit pas structuré de façon à favoriser le regroupement et le croisement de renseignements personnels, par exemple via l'instauration d'un identifiant unique qui y serait rattaché[27].

Si elle n'est pas adéquatement encadrée, cette production toujours plus importante de renseignements personnels est de surcroît synonyme de perte de contrôle des personnes sur leurs renseignements personnels et de risques accrus de fraude ou de vol d'identité.

Les modèles d'IN peuvent également soulever des craintes au niveau de la sécurité si les moyens déployés pour l'assurer s'avèrent insuffisants ou si un certain niveau de sécurité était sacrifié au profit d'une meilleure prise en main pour les usagers. De même, un choix d'architecture centralisée désignerait une cible unique pour les attaques et en aggraverait les impacts[28].

Au-delà des risques relevant de la protection de la vie privée et de la sécurité des systèmes d'IN, les risques d'exclusion et d'inégalité doivent être pris en compte. La population connaît des variations au niveau de l'accès aux technologies et, plus largement, au niveau de la littéracie

[25] L'authentification des personnes est basée une ou plusieurs de ces trois caractéristiques: ce que sait la personne, qui elle est, et ce qu'elle possède. Voir F. GARIÉPY et B. DUPONT, précité, note 8, p. 14.
[26] Voir GROUPE DE RECHERCHE INTERDISCIPLINAIRE EN CYBERSÉCURITÉ, précité, note 13, p. 9.
[27] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 14, p. 11.
[28] *Id.*, p. 13.

numérique. Cet état de fait risque de faire en sorte que seule une partie de la population adopte l'IN et bénéficie des avantages associés. L'adoption subséquente de politiques donnant la priorité au numérique au détriment des services en personne pourrait accentuer le fossé numérique et constituer *de facto* une inégalité sociale[29].

2.1.4. Les balises nécessaires dans le cadre d'un projet d'identité numérique pour assurer la protection des renseignements personnels

Dans les sections précédentes, il a été démontré que les promesses et les risques reliés à l'IN sont intimement liés et que le succès ou l'échec d'un système dépend de plusieurs choix de conception et de gouvernance. La saine gestion des renseignements personnels est au cœur de l'enjeu : pour tirer les bénéfices de l'IN, il faut d'abord assurer la protection de la vie privée des personnes et la sécurité de leurs renseignements personnels.

À cette fin, une approche respectueuse de la vie privée dès la conception et par défaut est indispensable. Cette approche doit mettre les personnes au centre des préoccupations, notamment par le déploiement de systèmes spécifiquement conçus pour répondre à leurs besoins et pour assurer leur protection, en plus de considérer leurs points de vue lors de la conception et du développement de l'IN. D'ailleurs, ces éléments sont propices à favoriser la confiance du public envers la nouvelle technologie qui lui est proposée et, partant, son adoption.

Afin de se conformer à cette approche, plusieurs éléments doivent être respectés tout au long du cycle de vie du système, que ce soit en matière de gouvernance, des caractéristiques du système, du respect des principes en matière de protection des renseignements personnels ou encore des garanties des droits des personnes. Plusieurs d'entre eux, essentiels, sont exposés ci-bas[30].

L'importance des phases préparatoires d'un projet d'IN nationale doit être soulignée. Considérant l'ampleur du changement représenté par l'IN ainsi que les enjeux associés, un déploiement réussi ne saurait faire l'économie de phases de consultations et d'évaluations abouties. À cet égard, il est nécessaire d'impliquer toutes les parties prenantes, y compris les citoyens, tout au long du processus, de la conception à la mise en application du système. Cette prise en considération des différents points de vue permet de faire ressortir les risques à prévenir, les moyens de les atténuer ainsi que les besoins auxquels il faut répondre. Notamment, les besoins spécifiques à l'utilisation de l'IN par les personnes mineures devraient être recensés et pris en compte dans le cadre réglementaire.

Dans la même veine, considérant la place centrale des renseignements personnels dans le cadre d'un système d'IN nationale, tout projet de ce genre doit faire objet d'une évaluation des facteurs

[29] F. GARIÉPY et B. DUPONT, précité, note 8, p. 13.

[30] La présente liste ne se veut pas exhaustive. Plusieurs documents font mention d'autres conditions, propriétés et principes à respecter dans le cadre du développement de systèmes d'IN gouvernementaux. Voir notamment COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX ET DES OMBUDSMANS QUI ASSUMENT UNE FONCTION DE SURVEILLANCE DANS LE DOMAINE, précité, note 21; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, précité, note 14; CONSEIL DE L'EUROPE, *Lignes directrices sur l'identité nationale numérique*, 2023, en ligne : <https://rm.coe.int/t-pd-2021-2rev9-fr-lignes-directrices-identite-numerique-2751-1821-338/1680a95e1f>; F. GARIÉPY et B. DUPONT, précité, note 8; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, précité, note 14.

relatifs à la vie privée détaillée et aboutie, où les risques pour la protection des renseignements personnels seraient identifiés, et où des mesures d'atténuation seraient prévues pour y répondre. Cette évaluation doit être réalisée en continu et suivre les phases de conception, de développement et de mise à jour du système.

Un encadrement clair et bien défini des utilisations possibles de l'IN pour toutes les parties prenantes doit être disponible avant sa mise en œuvre. Un système national d'IN ne doit servir qu'à des fins légitimes et nécessaires, et non à des fins justifiables uniquement par leur caractère souhaitable pour une partie prenante. En particulier, les utilisations pouvant causer préjudice aux personnes ou qui vont à l'encontre de leurs intérêts devraient être proscrites. C'est le cas du traçage et du profilage à leur insu qui pourraient être prévenus par des mesures visant à prévenir l'agrégation ou la conservation inutile de renseignements personnels et par la limitation de la possibilité d'opérer des croisements de données, notamment par le truchement d'identifiants uniques. Ces limites devraient être prévues législativement et être prises en compte dans la construction même du système.

Les systèmes d'IN devraient être interopérables. Cette caractéristique doit être assurée par voie technologique, mais aussi par l'adaptation conséquente des cadres réglementaires. De plus, l'IN devrait préserver la possibilité d'interagir avec les organisations de façon dite « pseudonyme ou anonyme » lorsqu'il n'y a pas nécessité pour la personne de produire son identité civile. Afin de réduire les risques de surveillance et de sécurité, les architectures centralisées, où tous les renseignements se trouvent dans une même base de données, devraient être évitées.

En ce qui a trait à la protection des renseignements personnels, quelques principes essentiels doivent guider la mise en œuvre de l'IN. Le principe de minimisation devrait être appliqué à toutes les étapes du processus numérique : seuls les renseignements personnels nécessaires doivent être collectés, utilisés, communiqués ou conservés. À cet égard, les renseignements biométriques ont une saillance particulière. Tout moyen d'authentification par la biométrie devrait être facultatif. De plus tout usage de la biométrie devrait être fait dans les strictes limites du principe de minimisation.

En plus de la minimisation, le système d'IN doit assurer que les personnes soient en contrôle. Le consentement exprès et éclairé devrait ainsi être à l'origine de toute communication entre les personnes et les organisations. Les personnes doivent avoir la maîtrise des attributs associés à leur IN et avoir le choix de ceux qu'elles partagent, à quel moment et à quelle organisation. Par surcroît, des mesures en matière de transparence doivent être assurées. Pour que le consentement soit valide, les personnes doivent notamment savoir à quelles fins leurs renseignements seront utilisés. Plus largement, elles doivent être au courant des répercussions potentielles sur leur vie privée des flux d'informations qui circulent au sein de l'écosystème d'IN.

Les personnes doivent également être au fait de leurs droits et des recours qui leur sont offerts en cas de problèmes ou de préjudices reliés au système d'IN ou à son utilisation. Notamment, les droits d'accès et à la rectification de ses renseignements personnels sont des conditions essentielles d'un système d'IN respectueux des personnes puisque la prestation des services offerts dépend de leur exactitude.

Enfin, considérant le degré variable de littéracie numérique au sein de la population, ainsi que le nombre de renseignements personnels que peut contenir l'IN et le potentiel inhérent de surveillance que ceci apporte, il importe que l'utilisation de l'IN soit volontaire et facultative. Par

conséquent, d'autres moyens d'identification auprès de l'administration publique doivent être offerts aux personnes. Ces moyens doivent être raisonnablement pratiques et accessibles. De même, la possibilité de recevoir des services en personne doit être maintenue. Par souci de combattre le fossé numérique et d'inclusion, des mesures d'assistance devraient être déployées pour venir en aide aux personnes éprouvant des difficultés à naviguer dans le monde numérique et qui souhaiteraient profiter des avantages de l'IN.

2.2. L'identité numérique ailleurs dans le monde

Plusieurs États à travers le monde ont déjà mis en place ou entamé des travaux visant à l'instauration d'IN nationale. Les initiatives de l'Australie et de l'Union européenne (UE), issues de travaux de longue haleine, sont parmi les plus avancées.

Le *Digital Act 2024* australien, adopté le 30 mai 2024, est entré en vigueur le 1er décembre de la même année[31]. Quant à l'Union européenne, des amendements au *Règlement eIDAS* (maintenant nommé eIDAS 2.0)[32] sont entrés en vigueur en octobre 2024 afin d'encadrer les portefeuilles numériques et de s'assurer de l'interopérabilité entre ceux des États membres. Ces deux initiatives visent à fournir des moyens sécuritaires facilitant la participation de la société au numérique et prévoient la participation du public comme du privé. Présentant de nombreuses similitudes, elles se démarquent tant par l'exhaustivité et la clarté de leurs cadres réglementaires que par les garanties qu'elles confèrent aux utilisateurs.

Cadre réglementaire

Les deux juridictions ont opté pour l'adoption de lois-cadres autoportantes, qui définissent clairement tous les termes associés à l'IN (respectivement 57 pour l'UE et 60 pour l'Australie). Ces lois prévoient l'encadrement du système et de l'écosystème d'IN. Elles assurent, avec les autres instruments réglementaires et normatifs dans leur giron, la clarté et la stabilité des systèmes avant même leur déploiement.

Le cadre européen prévoit ainsi l'établissement par la Commission européenne de normes de référence et de procédures concernant la mise en œuvre des portefeuilles numériques. Au total, 11 règlements concernant entre autres les fonctionnalités essentielles des portefeuilles, les attestations d'attributs et les données d'identification, de même que des spécificités techniques viennent préciser l'application de la loi. Du côté australien, la loi introduit un cadre pour la production de normes relatives à l'IN, dont deux ensembles sont présentement en vigueur. Deux règlements complémentent la loi.

Par surcroît, les lois renvoient explicitement aux pièces législatives encadrant la protection des renseignements personnels de leur juridiction respective : l'UE pour spécifier que le règlement s'applique sans préjudice du Règlement général sur la protection des données (RGPD), et l'Australie pour préciser que les mesures prévues au *Digital Act 2024* s'appliquent en sus de

[31] PARLEMENT AUSTRALIEN, *An Act to provide for the accreditation of entities in relation to digital IDs and to establish the Australian Government Digital ID System, and for related purposes*, 11 décembre 2024, en ligne : <https://www.legislation.gov.au/C2024A00025/latest> (consulté le 23 janvier 2025).

[32] PARLEMENT EUROPÉEN, *Règlement (EU) No 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*, en ligne : <https://eur-lex.europa.eu/eli/reg/2014/910/2024-10-18/eng> (consulté le 23 janvier 2025).

celles du *Privacy Act 1988*. La loi australienne précise d'ailleurs que tant qu'ils sont en possession ou sous le contrôle des entités accréditées, les attributs des personnes sont considérés en tant que renseignements personnels, même dans la mesure où ils ne correspondraient pas à la définition inscrite au *Privacy Act 1988*.

Écosystème

Les lois définissent les rôles et les obligations des diverses parties prenantes, qu'il s'agisse des administrateurs des systèmes, des régulateurs ou des autres entités participantes. Des mécanismes d'accréditation sont prévus pour assurer la conformité de ces dernières. En Europe, toute partie utilisant un portefeuille numérique doit être certifiée et enregistrée auprès de l'État membre, qui tient un registre public. L'Australie réserve ses accréditations à quatre types d'entités, dont les fournisseurs d'attributs et les fournisseurs de services d'identité. Les accréditations sont conditionnelles notamment au respect de mesures de protection des renseignements personnels et de normes techniques, ainsi qu'à la réalisation d'évaluation des facteurs de risques. Par surcroît, des sceaux de conformité (« Digital ID trustmark ») sont prévus pour les organisations participantes.

Pour ce qui a trait à la régulation, les deux juridictions optent pour l'implication de plusieurs acteurs à qui elles donnent le devoir de collaborer. Les États membres de l'UE doivent mettre en place des organes de contrôle des fournisseurs de portefeuilles et des fournisseurs de services, lesquels ont des pouvoirs d'inspection et d'enquête. L'Australie a désigné son autorité en matière de protection des consommateurs à titre de régulateur. Elle doit à ce titre promouvoir le respect de la loi et diffuser l'information sur son application. La loi prévoit explicitement qu'elle doit à ces fins consulter les autres agences gouvernementales impliquées dans l'écosystème d'IN, notamment le Commissaire à l'information[33], qui doit être avisé des sujets reliés à la protection de la vie privée et à qui les informations pertinentes doivent être partagées.

Administration

Les deux juridictions prévoient des obligations en matière de reddition de comptes. Au sein de l'UE, les États membres doivent colliger des statistiques annuellement concernant l'utilisation des portefeuilles numériques et la Commission européenne doit diffuser des listes des entités participantes. En Australie, le régulateur doit lui aussi diffuser des registres des entités accréditées et des organisations participantes. Il doit, de même que le Commissaire à l'information, remettre un rapport sur l'application de la loi.

Par surcroît, les lois prévoient la possibilité d'infliger des sanctions aux contrevenants. Notamment, le Commissaire à l'information australien reçoit explicitement les pouvoirs d'émettre des ordonnances et d'infliger des amendes.

Protection des renseignements personnels et contrôle des utilisateurs

Plusieurs mesures visant à assurer le contrôle des personnes sur leurs renseignements personnels sont prévues au sein même des lois européenne et australienne. Avant toute chose, elles établissent clairement le caractère volontaire de la participation au système d'IN.

[33] Le *Information Commissioner* est le responsable australien de la protection des renseignements personnels.

L'eIDAS 2.0 spécifie même que les personnes n'ayant pas recours à l'IN ne doivent pas être désavantagées dans l'accès aux services publics et privés et que la possibilité de s'identifier et de s'authentifier par d'autres voies demeure. Les deux lois prévoient également la possibilité pour les personnes de désactiver leur IN.

En matière d'utilisation de l'IN, l'eIDAS 2.0 met un fort accent sur la liberté de choix de l'individu, promettant un « contrôle total[34] » de la personne sur l'utilisation de son IN et sur les renseignements qui s'y trouvent. Ce contrôle se vérifie notamment par la possibilité d'effectuer un partage sélectif de ses attributs et par la préservation de la possibilité de l'utilisation de pseudonymes.

Le contrôle des personnes sur leurs renseignements personnels se traduit également par la mise en place de mesures restreignant leur collecte et leur utilisation par les autres entités impliquées dans le système d'IN. Le règlement européen prévoit à cet égard plusieurs mesures visant à minimiser la collecte et la combinaison de renseignements et à empêcher le profilage des personnes. Notamment, les fournisseurs de portefeuilles ne peuvent collecter des informations non nécessaires à l'utilisation de ceux-ci et ils ne peuvent combiner de renseignements avec d'autres provenant d'autres services. Les fournisseurs d'attestations ont eux aussi l'interdiction, après la délivrance des attestations, d'obtenir des données permettant le traçage et le profilage.

L'eIDAS 2.0 prévoit enfin qu'un tableau de bord soit mis à la disposition des personnes afin qu'elles puissent avoir accès à la journalisation des utilisations, signaler toute demande suspecte et demander la suppression de ses renseignements personnels détenus par une organisation en vertu des dispositions du RGPD.

En ce qui concerne le contrôle, le *Digital Act 2024* exige quant à lui le consentement exprès pour la communication d'attributs reliés à l'identité civile ou à d'autres renseignements sensibles établis dans les règles d'accréditation. La loi australienne prévoit également plusieurs mesures restreignant la collecte et l'utilisation de renseignements personnels par d'autres entités. Notamment, les entités accréditées ne peuvent collecter volontairement de renseignements personnels sensibles pouvant constituer des motifs de discrimination, par exemple l'origine ethnique ou l'affiliation politique de la personne. En matière de profilage, les entités accréditées ne peuvent communiquer ou utiliser de renseignements personnels permettant de tracer les personnes, tels que les services auxquels la personne a accédé, à quel moment et par quelle façon, et ce, même si la personne y a consenti. L'utilisation ou la communication de renseignements personnels à des fins de marketing est elle aussi proscrite. La loi impose également des restrictions aux entités accréditées au niveau de la collecte et de l'utilisation de renseignements biométriques. En règle générale, les entités accréditées peuvent se servir de ces renseignements qu'à des fins d'identification ou de vérification de l'identité, et ce, si leurs conditions d'accréditation le permettent. Pour toute autre fin que celles prévues par la loi, les entités doivent obtenir préalablement le consentement explicite de la personne. La loi encadre également la destruction de ces renseignements. Notamment, les entités qui ne s'en servent que pour vérifier l'identité d'une personne doivent les supprimer immédiatement après l'usage.

[34] Règlement eIDAS 2.0, art. 5 bis (14).

2.3. Analyse des dispositions du projet de loi nº 82 concernant l'identité numérique

La Commission a présenté, dans les sections précédentes de son mémoire, les principaux éléments devant, selon elle, être considérés en matière d'IN et de protection des renseignements personnels. C'est en s'appuyant sur ces éléments que la Commission souhaite commenter les dispositions relatives à l'IN prévues dans le projet de loi.

Dans le cadre de cet exercice, la Commission comprend que le projet de loi est une première étape législative qui vise à introduire une IN nationale au Québec. Par exemple, le rôle des acteurs de la sphère privée est inexistant dans le projet de loi et une modification législative sera nécessaire pour introduire ceux-ci.

Dans ses commentaires, la Commission prend également en considération le fait que la législation québécoise contient déjà des règles, obligations, responsabilités ou normes qui trouveront applications en matière d'IN. Par exemple, la Loi sur l'accès ainsi que la Loi sur la protection des renseignements personnels dans le secteur privé[35] s'appliquent en matière de protection des renseignements personnels et la LCCJTI s'applique également en matière de valeur juridique et d'intégrité des documents ainsi qu'en matière de biométrie aux fins de vérifier ou de confirmer l'identité.

Bien que le projet de loi contienne certaines normes, comme l'interdiction pour le ministre d'utiliser les renseignements du registre de l'IN nationale à des fins de profilage ou comme les Règles relatives à l'assurance de l'identité numérique, celles-ci semblent insuffisantes.

Dans ce contexte, la Commission ne peut se prononcer de manière complète sur la question de la protection des renseignements personnels en lien avec l'IN nationale puisque l'écosystème présenté dans le projet de loi est selon elle incomplet. En effet, la lecture du projet de loi ne permet pas de comprendre clairement le fonctionnement de l'IN. Notamment, la Commission est d'avis que le cadre normatif global du projet de loi est nettement insuffisant pour assurer :

- L'encadrement de l'IN nationale;
- La sécurité globale de l'écosystème de l'IN nationale;
- L'interopérabilité des systèmes d'IN nationale;
- La protection des renseignements personnels;
- Le contrôle des citoyens sur les attributs de leur identité;
- La possibilité pour les citoyens d'entreprendre des recours ou pour une autorité de surveillance d'effectuer des enquêtes et de sanctionner des comportements contraires au cadre de l'IN nationale.

La Commission souligne que selon sa compréhension du projet en ressources informationnelles d'intérêt gouvernementale Service québécois d'identité numérique (SQIN) - bloc identité numérique citoyenne, des éléments identifiés comme manquant au projet de loi sont prévus dans

[35] *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ, c. P-39.1, ci-après, la Loi sur le privé.

ce projet. C'est donc avec une certaine surprise que la Commission constate que certains de ces éléments ne se trouvent pas au projet de loi.

2.3.1. L'encadrement de l'identité numérique nationale dans le projet de loi

L'IN est susceptible de générer des quantités importantes de renseignements, dont des renseignements particulièrement sensibles. L'encadrement insuffisant d'un système d'IN peut mener à des dérives importantes et à des risques significatifs en matière de protection des renseignements personnels. Or, la Commission constate que le projet de loi rend difficile la conceptualisation du système d'IN qui sera effectivement mis en place, ce qui en soit est problématique et rend difficile l'évaluation des garanties concernant la protection des renseignements personnels qu'offre réellement le projet d'IN nationale.

La définition de l'identité numérique au projet de loi manque de clarté

La Commission est d'avis que le concept d'IN nationale défini à l'article 10.2 de la LMCN[36] est trop large et qu'il incorpore sous un même terme trop d'éléments pourtant distincts. En somme, l'utilisation d'un terme unique dans le projet de loi mène à une certaine confusion générale quant au contour de l'IN nationale.

Par exemple, l'arrêté numéro 2024-03 du 6 juillet 2024 du ministre de la Cybersécurité et du Numérique prévoit des Règles relatives à l'assurance de l'identité numérique. Cet arrêté définit à l'article 4 ce qu'est une « équivalence des identités », soit que « l'identité d'une personne et l'IN d'une telle personne sont équivalentes ». Cette définition soulève une ambiguïté avec ce qui est prévu au premier alinéa de l'article 10.2. Ce dernier prévoit que l'IN représente l'ensemble des moyens dont dispose l'État pour garantir à toute personne un accès sécurisé aux prestations électroniques de services gouvernementaux et lui permettre d'avoir un niveau de confiance élevé lors de ses interactions avec les organismes publics. En ce sens, la Commission se demande comment un « ensemble de moyens » peut-il être équivalent à l'identité d'une personne?

De plus, la Commission comprend que l'expression « niveau de confiance élevé » utilisée au premier alinéa de cet article fait référence au sentiment de sécurité du citoyen lors de ses interactions avec les organismes publics. Mais cette expression, en raison des termes qui s'y trouvent, sème une certaine confusion avec des concepts reconnus et spécifiques à l'identification et à l'authentification. Par exemple, les Règles relatives à l'assurance de l'identité numérique prévues à l'arrêté 2024-03 qui réfèrent, notamment, aux exigences relatives à l'identification et à l'authentification, lesquelles doivent offrir un « degré de confiance » suffisant pour la prestation du service concerné[37] et aux « niveaux d'assurance » de l'identité.

Également, la Commission comprend que l'utilisation du terme « collectivité » à cet article permet l'ouverture de l'utilisation de l'IN par les citoyens dans le secteur privé.

[36] Édicté par l'article 6 du projet de loi.
[37] Article 1 al. 2 des Règles relatives à l'assurance de l'identité numérique.

La Commission se permet aussi de souligner qu'il semble que l'expression « prestations de services gouvernementales » qui se trouve à cet article devrait plutôt être « prestation de services gouvernementaux »[38].

Recommandation 01 : la Commission estime que la définition de l'IN nationale doit être clarifiée et que les termes utilisés dans le chapitre I.1 de la LMCN ne doivent pas susciter d'ambiguïté avec les termes utilisés dans les autres documents relatifs à l'IN nationale, comme les Règles relatives à l'assurance de l'identité numérique.

Les parties prenantes de l'identité numérique nationale ne sont pas définies et leurs obligations ne sont pas encadrées

La Commission constate que les parties prenantes de l'IN nationale ne sont pas définies et que l'encadrement de ces dernières est absent du projet de loi.

Comme nous l'avons mentionné précédemment, un système d'IN nécessite la mise en place d'un triangle de confiance qui repose sur trois acteurs :

1) **Le détenteur de l'attestation :** représente le citoyen qui souhaite accéder à un service et qui doit fournir des preuves de son identité au fournisseur de service;
2) **L'émetteur de l'attestation** : représente un tiers de confiance, fournisseur d'identité, qui émet l'attestation qui permet au fournisseur de vérifier l'authenticité des attestations, notamment via la consultation d'un registre de preuve;
3) **Le vérificateur (ou consommateur) :** représente un fournisseur de service qui doit vérifier l'authenticité des attestations du citoyen (détenteur) avant de fournir son service.

Le projet de loi est muet quant à ces trois acteurs essentiels de tout projet d'IN. La Commission s'interroge sur la façon dont on peut assujettir ces acteurs à des normes législatives ou réglementaires, notamment à un cadre de confiance tel que mentionné ci-dessous, s'ils ne sont pas décrits au projet de loi. De même, la Commission est d'opinion que les obligations de ces acteurs de premier plan devraient être prévues autrement que dans un cadre contractuel.

Recommandation 02 : la Commission recommande de décrire au projet de loi les acteurs du triangle de confiance, soit le détenteur, l'émetteur et le vérificateur.

L'encadrement des utilisations possibles des renseignements relatifs à l'identité numérique nationale devrait être mieux défini

L'encadrement des utilisations possibles des renseignements, personnels ou non, relatifs à l'IN nationale n'est pas suffisant. En fait, le troisième alinéa de l'article 10.7 de la LMCN[39] est la seule disposition qui prévoit une interdiction pour le ministre d'utiliser les données du registre de l'IN

[38] Voir « terme utilisé dans certains contextes », Grand dictionnaire terminologique (2003), en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8870634/prestation-de-services#:~:text=Lorsque%20le%20contexte%20exige%20plus%20de%20pr%C3%A9cisions%2C%20on,expression%20incorrecte%20pour%20d%C3%A9signer%20une%20prestation%20de%20services> (consulté le 21 janvier 2025). Cette expression se trouve aussi à l'article 10.3 de la LMCN, édicté par l'article 6 du projet de loi.

[39] Édicté par l'article 6 du projet de loi.

nationale à des fins de profilage. La Commission estime que cette interdiction n'est pas suffisamment large.

La Commission y reviendra plus loin, mais précise ici qu'à son avis, il n'est pas souhaitable que le ministre utilise les données pour des utilisations secondaires comme le permet la Loi sur l'accès en certaines circonstances. La Commission propose de limiter plus amplement l'usage du registre par le ministre. Outre les utilisations nécessaires à l'exercice des fonctions prévues au chapitre I.1 de la LMCN, la Commission est d'avis que le projet de loi devrait également interdire à qui que ce soit toute utilisation secondaire des données relatives au registre de l'IN nationale.

> **Recommandation 03 : la Commission recommande que le projet de loi interdise au ministre et à toute organisation publique ou privée d'utiliser les données contenues au registre de l'IN nationale à une fin autre que celles nécessaires à l'exercice des fonctions prévues au chapitre I.1 de la LMCN.**

L'encadrement des attestations d'identité devrait être établi

L'encadrement des attestations est inexistant au projet de loi.

En effet, l'article 10.2 de la LMCN[40] introduit « l'attestation numérique gouvernementale », qui est contrôlée par une personne à partir d'une application où elle est déposée de façon sécurisée. Cette « attestation numérique gouvernementale » est décrite comme étant un « document technologique permettant d'établir l'authenticité ou la véracité d'une information ou d'un fait se rapportant à une personne ».

Outre ces mentions, le projet de loi n'émet aucun principe ni encadrement relatif au déploiement, à l'utilisation, à la conservation ou au contrôle des attestations. L'une des caractéristiques principales de l'IN et de l'utilisation d'une attestation est la possibilité, pour une personne, de ne divulguer ou de ne présenter que les renseignements personnels nécessaires à l'obtention d'une prestation de service. En certaines circonstances, une attestation peut même ne dévoiler aucun renseignement personnel en confirmant simplement un fait (la majorité, par exemple).

La Commission estime qu'il est essentiel que le projet de loi encadre la vérification des attestations afin d'obliger les acteurs du système d'IN nationale, principalement l'émetteur, à minimiser la divulgation des renseignements personnels contenus dans les attestations. En principe, une attestation ne devrait divulguer ou présenter que le minimum de renseignements personnels requis, ou même aucun renseignement personnel lorsque cela est possible, pour l'obtention de la prestation de service demandé par le détenteur de l'attestation.

De plus, la Commission rappelle que la Loi sur l'accès et la Loi sur le privé prévoient une obligation d'information[41] relative à la collecte et à l'utilisation de renseignements personnels. À cet égard, la Commission est d'avis que le projet de loi devrait prévoir que toute vérification d'une attestation ainsi que toute collecte de renseignement à partir d'une attestation devraient être effectuées avec le consentement exprès du détenteur de cette attestation. Le consentement exprès nécessite que le détenteur de l'attestation pose un geste positif pour accepter la

[40] Édicté par l'article 6 du projet de loi.
[41] Loi sur l'accès, précité note 18, article 65 à 65.0.2 et Loi sur le privé, précité note 35, article 8 à 8.3.

vérification de son attestation. Selon le cas, le détenteur d'une attestation devrait pouvoir déterminer laquelle de ses attestations sera soumise à la vérification. Ce n'est que de cette façon que le citoyen exercera un réel contrôle de ses attestations.

Recommandation 04 : la Commission recommande :

- **Que le projet de loi prévoie que la vérification d'une attestation ne doit permettre que la divulgation minimale de renseignements personnels selon le contexte de la vérification effectuée. Au surplus, toute modalité requise à cet égard devrait être prévue par voie réglementaire (cadre de confiance);**

- **Que le projet de loi oblige l'obtention d'un consentement exprès du détenteur d'une attestation et qu'il permette à celui-ci, dans les cas où cela est possible, de déterminer l'attestation à présenter. Toutes les modalités relatives au consentement devraient être prévues par les règlements du ministre.**

2.3.2. Les recours et sanctions dans le projet de loi

La Commission est d'avis que des dispositions comportant des recours et des sanctions doivent être ajoutées au projet de loi.

Le projet de loi devrait prévoir des recours pour les citoyens

Le projet de loi ne prévoit pas de recours clair pour les citoyens. Ils doivent disposer de recours en cas de problèmes ou de préjudices liés au système de l'IN ou à son utilisation. Ils doivent également être informés de leurs droits et de ces recours**.**

Recommandation 05 : la Commission recommande l'ajout de recours pour les citoyens au projet de loi.

Le projet de loi devrait prévoir des sanctions pour la contravention du cadre normatif de l'identité numérique nationale

Le projet de loi ne prévoit pas de sanction pour la contravention au cadre normatif qui sera applicable aux acteurs de l'écosystème de l'IN. La Commission considère essentiel l'ajout d'obligations claires au projet de loi relativement aux obligations des différents acteurs impliqués dans l'IN. Le non-respect de ces obligations doit être sanctionnable pour favoriser la confiance de la population et maximiser la conformité aux règles en vigueur.

Recommandation 06 : la Commission recommande l'ajout de sanctions pour la contravention du cadre normatif de l'IN nationale. Plus spécifiquement, la Commission suggère d'ajouter une infraction correspondant au non-respect des obligations imposées aux différents acteurs de l'écosystème de l'IN.

Le projet de loi devrait prévoir des mesures de protection supplémentaires concernant le profilage, la surveillance et le traçage

La Commission suggère d'ajouter au projet de loi qu'effectuer du profilage, du traçage ou de la surveillance à l'aide de l'IN nationale ou des renseignements qui découlent de son utilisation est interdit et constitue une infraction. En effet, la Commission est d'avis que l'IN ne devrait d'aucune

façon permettre à qui que ce soit de profiler les individus qui l'utilisent ou de les surveiller. À cet égard, la Commission recommande que le projet de loi interdise à tous les organismes publics ainsi qu'à toutes les organisations privées d'utiliser les renseignements qui pourraient découler de l'utilisation de l'IN nationale à des fins de profilage ou de surveillance des citoyens.

De plus, le projet de loi est muet en ce qui concerne le traçage et la géolocalisation. La Commission propose d'ajouter des limites législatives claires et plus exhaustives relativement aux données contenues et résultant du système de l'IN.

Recommandation 07 : la Commission recommande

- **D'ajouter une interdiction pour les organisations privées et les organismes publics d'effectuer du profilage, du traçage ou de la surveillance à l'aide de l'IN nationale ou des renseignements qui découlent de son utilisation et que le non-respect de cette interdiction constitue une infraction[42].**
- **Que le projet de loi contienne des restrictions claires et précises concernant l'interdiction de tracer ou surveiller les citoyens eux-mêmes, mais également les transactions effectuées par les citoyens à l'aide de l'IN ou d'effectuer des activités de géolocalisation avec ces mêmes données.**

2.3.3. Le cadre normatif de l'identité numérique nationale dans le projet de loi

Comme cela a été mentionné précédemment, un système d'IN est susceptible de contenir et de générer une quantité importante de renseignements personnels. Il va de soi que des règles robustes, dont des mesures de sécurité, sont nécessaires.

Le projet de Loi devrait établir clairement le cadre normatif applicable à l'écosystème de l'identité numérique nationale

D'une part, la Commission est d'avis que le projet de loi devrait contenir des notions ou des principes relatifs aux mesures de sécurité. En effet, il est frappant de constater que le mot « sécurité » ne se retrouve à aucune des dispositions des articles 10.2 à 10.10 de la LMCN[43]. D'autre part, le cadre de confiance ou le cadre normatif applicable aux acteurs de l'IN nationale est insuffisant.

En ce sens, il est intéressant de constater que l'article 5 des *Règles relatives à l'assurance de l'identité numérique* réfère au Cadre de confiance pancanadien du Conseil canadien de l'identification et de l'authentification numériques[44]. Or, l'assurance de l'IN n'est qu'une infime partie de l'ensemble des règles normatives à mettre en place pour assurer la viabilité, la fiabilité, la transparence et la sécurité de l'écosystème de l'IN nationale.

Considérant la nature technique de ce type d'encadrement, la Commission comprend que de telles règles ne soient pas inscrites dans le projet de loi, mais la plupart de celles-ci sont

[42] COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE FÉDÉRAL, PROVINCIAUX ET TERRITORIAUX ET DES OMBUDSMANS QUI ASSUMENT UNE FONCTION DE SURVEILLANCE DANS LE DOMAINE, précité, note 21.
[43] Édicté par l'article 6 du projet de loi.
[44] En ligne : https://diacc.ca/fr/trust-framework-fr/.

indispensables à la mise en place d'un système complet d'IN. Dans ce contexte, la Commission estime que non seulement le ministre doit adopter toutes les règles nécessaires, mais que le projet de loi devrait identifier les normes opérationnelles minimales requises avant le déploiement d'un système d'IN nationale. Par exemple, la Commission estime qu'il est indispensable que des règles relatives à la mise en place d'un registre des preuves soient en vigueur avant toute utilisation d'une attestation émise par un organisme public.

> **Recommandation 08 : la Commission recommande que le projet de loi identifie les normes opérationnelles minimales requises avant le déploiement de l'IN nationale dans les organismes publics, afin que le ministre adopte les règles conséquentes à ces normes minimales.**

De plus, l'article 10.4 prévoit notamment que le ministre assume la responsabilité de la gouvernance et de la gestion centralisée de l'IN nationale et lui octroie certains pouvoirs à ces fins. La Commission comprend de cet article que l'utilisation de l'expression « gestion centralisée » n'équivaudrait pas à la mise en place d'une base de données centralisée. La Commission est d'avis qu'il faut éviter, dans tous les cas où cela est possible, de telles bases de données centralisées dans le cadre de l'IN nationale.

Le projet de loi devrait prévoir l'implication de toutes les parties prenantes à l'identité numérique, tout au long du processus

Le projet de loi ne prévoit pas l'implication des parties prenantes tout au long du processus de l'élaboration et de la mise en œuvre de l'IN. Considérant l'évolution des technologies, la Commission propose d'ajouter au projet de loi une disposition prévoyant une révision périodique de cette loi. Une telle disposition pourrait également prévoir des consultations publiques périodiques ou, à tout le moins, des consultations ciblées d'experts du domaine des technologies (cybersécurité, protection des renseignements personnels, etc.). Un tel ajout favoriserait une plus grande transparence. La Commission considère qu'il est important pour la population d'avoir l'opportunité de donner son avis périodiquement sur l'évolution de l'IN. De plus, puisque l'IN est un concept complexe et en développement constant, cet ajout permettrait de s'assurer que la loi est adaptée au contexte technologique.

> **Recommandation 09 : la Commission recommande d'ajouter au projet de loi une obligation de révision périodique, laquelle pourrait inclure une consultation publique.**

Le projet de loi devrait prévoir un cadre de surveillance de l'application de la loi par un organisme indépendant

Le projet de loi ne prévoit pas la surveillance de l'application de la loi par un organisme indépendant. La Commission considère qu'il est essentiel qu'une disposition prévoyant qu'un organisme indépendant assure la surveillance des dispositions relatives à l'IN nationale soit ajoutée au projet de loi. Cet organisme doit disposer des ressources suffisantes pour effectuer adéquatement ce travail de surveillance.

D'ailleurs, la Loi modifiant principalement la Loi sur l'instruction publique et édictant la Loi sur l'Institut national d'excellence en éducation[45] a introduit le système de dépôt et de communication de renseignements en éducation[46]. C'est la Commission qui est chargée de surveiller l'application des dispositions relatives au système de dépôt et de communication de renseignements ainsi qu'à l'utilisation et à la communication de renseignements personnels[47].

En ce sens, la Commission souligne être notamment responsable de surveiller l'application de la Loi sur le privé, de la Loi sur l'accès et de la Loi sur les renseignements de santé et de services sociaux,[48] mais ne saurait insister suffisamment sur le fait que tout ce qui découle de l'IN nationale ne relève pas uniquement de la protection des renseignements personnels.

Par exemple, l'article 10.3 interdit à tous les organismes publics d'imposer à une personne l'utilisation de l'IN nationale. La Commission n'aurait aucun pouvoir d'intervention si un organisme public décidait d'imposer l'IN nationale dans le cadre de la dispensation de l'un de ses services.

Recommandation 10 : la Commission recommande qu'un organisme indépendant soit désigné afin de surveillance l'application du chapitre I.1 de la LMCN.

2.3.4. L'interopérabilité des systèmes d'identité numérique nationale dans le projet de loi

L'encadrement de l'interopérabilité des systèmes devrait être mieux défini

Le deuxième alinéa de l'article 10.8 prévoit que le gouvernement peut déterminer les conditions et modalités relatives aux ententes des organismes publics pour l'interopérabilité de l'IN nationale. La Commission est d'avis que le projet de loi devrait prévoir que le gouvernement doit déterminer les conditions essentielles qui doivent être contenues aux ententes que pourront conclure les organismes publics en matière d'interopérabilité. Certaines de ces conditions devraient se retrouver directement dans le projet loi. Par exemple, si une entente est conclue avec une organisation privée en lien avec la réalisation d'interactions (article 10.2 al. 2 de la LMCN), l'entente devrait prévoir que cette organisation est tenue en tout ou en partie au respect du cadre normatif applicable à l'IN nationale.

Également, la Commission est d'avis que le projet de loi doit prévoir que le défaut de respecter ces règles par une partie à une entente constitue une infraction. Ceci assure un certain seuil de protection et une certaine cohérence dans les ententes à être conclues.

Recommandation 11 : la Commission recommande de prévoir au projet de loi que le gouvernement doit prévoir les conditions et modalités relatives aux ententes des organismes publics pour l'interopérabilité de l'IN nationale.

[45] L.Q. 2023, c. 32.
[46] *Loi sur le ministère de l'Éducation, du Loisir et du Sport*, RLRQ, c. M-15, article 6.1.
[47] *Ibid.*, article 6.18.
[48] *Loi sur les renseignements de santé et de services* sociaux, RLRQ, c. R-22.1; ci-après, la LRSSS.

2.3.5. La protection des renseignements personnels dans le projet de loi

L'IN permet de favoriser la protection des renseignements personnels si les éléments requis sont mis en place. La Commission souligne qu'il s'agit d'une occasion de rehausser la protection des renseignements personnels qui doit être saisie.

Le projet de Loi devrait expressément référer au principe de la nécessité et de la minimisation concernant les attributs de l'identité

La divulgation minimale des renseignements personnels dans le cadre d'un système d'IN est à la fois un principe fondamental en matière de protection des renseignements personnels, mais surtout l'un des principaux avantages de l'IN pour les citoyens. Comme nous l'avons déjà mentionné dans la section relative à l'encadrement des attestations, le projet de loi ne contient aucune notion, principe ou obligation relative à la divulgation minimale des renseignements personnels ou même à l'absence de divulgation de renseignements personnels lorsque cela est possible.

Le projet de loi devrait davantage favoriser la protection des renseignements personnels dès la conception

Le projet de loi est peu éclairant quant à la protection des renseignements personnels dès la conception. L'article 10.5 prévoit notamment que le ministre fournit aux organismes publics les services relatifs à l'IN nationale qu'il détermine. La Commission n'a pas de commentaire sur l'attribution spécifique de cette fonction au ministre, mais elle souligne que le projet de loi demeure muet quant aux services qui seront dans les faits fournis par le ministre. Pourtant, le Service d'authentification gouvernementale et le Service québécois d'identité numérique sont annoncés et réalisés ou en phase d'exécution selon le cas. Cependant, ils ne sont pas nommés expressément au projet de loi.

La Commission n'est donc pas en mesure d'évaluer ni d'anticiper les impacts des services en matière de protection des renseignements personnels qui ne sont pas annoncés à ce jour. Or, il est primordial que l'évaluation de la protection des renseignements personnels soit réalisée dès la conception de chacun des services relatifs à l'IN nationale qui seront mis en place par le ministre.

2.3.6. Le contrôle des citoyens de leurs renseignements personnels et de leurs attestations dans le projet de loi

Comme précédemment mentionné, le système de l'IN doit permettre que les personnes aient un meilleur contrôle de leurs renseignements personnels. La Commission est d'avis qu'il ne ressort pas clairement du projet de loi que les citoyens détiennent un réel contrôle sur leurs renseignements.

Le projet de loi devrait prévoir qu'un registre des transactions doit être rendu disponible aux détenteurs

Aux fins de transparence du système et afin de permettre un meilleur contrôle des détenteurs d'identité sur la collecte et l'utilisation de leurs attributs, la Commission considère important qu'un registre des transactions soit rendu disponible aux détenteurs. Ce registre permettrait à ceux-ci d'avoir une vue d'ensemble sur les consommateurs qui ont accès à leurs attributs de l'identité, le tout afin d'assurer l'exercice et le suivi d'un consentement éclairé.

> **Recommandation 12 : la Commission recommande qu'un droit d'accès à un registre des transactions soit prévu au projet de loi.**

L'interdiction d'imposer l'utilisation de l'identité numérique nationale afin de recevoir des services d'un organisme public devrait être élargie

L'article 10.3 prévoit que l'utilisation de l'IN nationale ne peut pas être imposée par un organisme public à une personne afin de fournir à cette dernière une prestation de services gouvernementale. La Commission considère que cette interdiction doit être élargie afin que les organismes publics ne puissent jamais imposer l'utilisation de l'IN nationale. Par exemple, un corps policier ne devrait pas pouvoir imposer l'utilisation de l'IN à des fins d'identification d'une personne qu'il interpelle. Au surplus, la Commission estime que le projet de loi doit obliger les organismes publics à offrir d'autres moyens d'identification raisonnablement pratiques et accessibles.

> **Recommandation 13 : la Commission recommande que l'imposition de l'IN nationale soit interdite en tout temps. De plus, l'article 10.3 du projet de loi devrait prévoir que les organismes publics doivent offrir d'autres moyens d'identification raisonnablement pratiques et accessibles.**

Le projet de loi devrait établir comment les citoyens exerceront le contrôle de l'utilisation des attestations numériques contenues dans leur portefeuille d'identité

La Commission se questionne sur comment s'exerce le contrôle d'une personne sur les attestations numériques incluses dans son portefeuille numérique. La Commission est d'avis que ce concept devrait être davantage expliqué dans le projet de loi et non uniquement mentionné dans la définition de l'IN.

Le consentement des détenteurs d'attestations d'identité devrait être explicite

De plus, la Commission est d'avis que le consentement devrait être manifesté de manière expresse, c'est-à-dire que les personnes doivent poser un geste actif, ce qui se distingue de ce qui est prévu à la Loi sur l'accès ou à la Loi sur le privé. Les individus doivent également être en mesure de retirer leur consentement s'ils le souhaitent. Ceci favorise un meilleur contrôle des individus sur leurs renseignements personnels.

> **Recommandation 14 : la Commission recommande d'expliquer davantage le concept de contrôle des citoyens et de prévoir au projet de loi que le consentement doit être exprès et qu'il peut être retiré en tout temps.**

2.3.7. La clarté, la compréhension et la transparence du projet de loi

La Commission tient à rappeler l'importance de dispositifs qui favorisent la clarté et la transparence afin que l'IN puisse être comprise par la population. La Commission est d'avis qu'en raison de la complexité de l'IN, il est souhaitable d'ajouter un devoir d'information pour le ministre à l'égard de la population. Ceci favorise la confiance et la transparence qui sont des ingrédients clés pour le succès de l'implantation d'une IN. Une obligation similaire existe dans la LRSSS[49].

Recommandation 15 : la Commission recommande d'ajouter au projet de loi une obligation du ministre d'informer la population, notamment quant aux risques liés à l'utilisation de l'IN nationale et aux mesures à prendre pour en assurer la protection.

Le projet de loi gagnerait à être davantage clair, compréhensible et transparent relativement aux implications de l'identité numérique nationale

La Commission est d'avis que les notions, principes ou obligations manquants et soulignés dans les points précédents affectent la clarté du projet de loi et du système d'IN qu'il prévoit. La Commission ne retrouve pas dans ce projet de loi plusieurs concepts, notions, principes ou obligations qu'elle retrouve généralement dans des lois similaires développées par d'autres juridictions.

Outre les éléments déjà soulevés, la Commission constate que le projet de loi est laconique quant aux renseignements qui sont communiqués et détenus par le ministre.

À cet égard, l'article 6 prévoit notamment que le ministre agit d'office comme source officielle de données numériques gouvernementales aux fins de l'IN nationale. La Commission est satisfaite que le projet de loi prévoie une source officielle de nature législative et que certaines données numériques gouvernementales soient prévues de façon spécifique au projet de loi[50].

En revanche, la Commission est d'avis que le projet de loi doit prévoir l'ajout d'une disposition équivalente à l'article 12.11 de la LGGRI. Cet article prévoit que les pouvoirs du présent chapitre, soit celui portant sur les données numériques gouvernementales, doivent être exercés de manière à respecter le droit à la vie privée et le principe de transparence ainsi qu'à promouvoir la confiance du public dans les mesures permettant d'assurer la sécurité, la confidentialité, la disponibilité et l'intégrité des données numériques gouvernementales.

Ensuite, la Commission tient à souligner que toutes les données numériques gouvernementales ne se trouvent pas dans la loi telle que proposée. En effet, il s'agit uniquement d'une partie des données numériques gouvernementales puisque le décret 870-2022 du 25 mai 2022 prévoit certaines données numériques gouvernementales[51]. Ce décret est réputé pris conformément à l'article 10.6 en vertu de l'article 39 du projet de loi. L'article 40 du projet de loi prévoit que le registre d'attributs d'identité gouvernemental visé par ce décret devient le registre de l'IN

[49] LRSSS, précité note 48, article 280 : Le ministre doit, avant l'entrée en vigueur des articles 7 à 9, informer la population des droits de restriction et de refus qui y sont prévus.
[50] Article 10.6 al. 4 de la LMCN, édicté par l'article 6 du projet de loi.
[51] Il s'agit : du nom, du nom du mari (pour les femmes mariées avant le 2 avril 1981), de la date de naissance, de la date du décès, de l'adresse de résidence et de son historique, de l'indicateur de présence d'un répondant, du numéro d'assurance maladie, du numéro d'assurance sociale et son historique et de l'identifiant sectoriel de la Régie de l'assurance maladie du Québec.

nationale visé à l'article 10.7 de la LMCN édicté par l'article 6. Ainsi, les données numériques gouvernementales prévues dans ce décret ne se retrouvent pas dans la loi projetée.

La Commission est d'avis que toutes les données numériques gouvernementales déjà déterminées devraient être mentionnées au projet de loi pour plus de clarté et de transparence. La Commission s'explique mal le recours au décret 870-2022 du 25 mai 2022 alors que les données qui y sont prévues pourraient être ajoutées au projet de loi.

Finalement, la Commission constate que l'article 40 du projet de loi prévoit que le registre d'attributs d'identité gouvernemental visé par le décret 870-2022 du 25 mai 2022 devient le registre de l'IN nationale. La Commission est d'avis que le contenu du registre doit être prévu au chapitre I.1 de la LMCN. Il s'agit d'une question de transparence envers les citoyens susceptibles d'utiliser l'IN nationale. Néanmoins, la Commission est satisfaite de constater qu'aucun mécanisme n'est prévu au projet de loi pour modifier le contenu du registre.

Quant au contenu du registre, la Commission se questionne et doute fortement de la nécessité que celui-ci contienne des données telles que le numéro d'assurance maladie ou le numéro d'assurance sociale.

Recommandation 16 : la Commission recommande :

- **Que toutes les données numériques gouvernementales connues soient identifiées directement au projet de loi plutôt que par référence au décret 870-2022 du 25 mai 2022;**
- **Que le contenu du registre de l'IN nationale soit prévu au chapitre I.1 de la Loi;**
- **Qu'une disposition équivalente à l'article 12.11 de la LGGRI soit ajoutée au projet de loi.**

L'étendue du pouvoir réglementaire attribué par le projet de loi a un impact sur son niveau de transparence

L'article 10.9 prévoit une partie des pouvoirs réglementaires du gouvernement. La Commission est d'avis que certains pouvoirs réglementaires prévus à cet article sont trop vastes. Tout d'abord, la catégorie résiduaire permettant au gouvernement de réglementer sur toute autre mesure nécessaire[52] semble particulièrement large, compte tenu de la sensibilité de ce qui relève de l'IN. La Commission propose de retirer ce pouvoir réglementaire résiduaire du projet de loi.

Ensuite, cet article prévoit que le gouvernement peut par règlement déterminer les normes de qualité des données numériques gouvernementales et, le cas échéant, des normes de protection particulières[53]. Ce libellé est similaire au pouvoir prévu au premier paragraphe de l'article 12.21 de la LGGRI. Ces deux libellés semblent correspondre au même pouvoir et la Commission se questionne sur la nécessité de reproduire celui-ci au chapitre I.1 de la LMCN puisque le pouvoir prévu à la LGGRI vise déjà les données numériques gouvernementales. Si le pouvoir prévu au paragraphe 2° de l'article 10.9 vise uniquement les données numériques gouvernementales dont

[52] Article 10.9 al. 1 par. 4 de la LMCN, édicté par l'article 6 du projet de loi.
[53] Article 10.9 al. 1 par. 2 de la LMCN, édicté par l'article 6 du projet de loi.

il est question au chapitre I.1 de la LMCN, une précision à cet égard apporterait plus de clarté. Autrement, la Commission ne voit pas l'utilité de ce pouvoir réglementaire.

Également, cet article prévoit que le gouvernement peut par règlement 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[54]. La biométrie touche les renseignements les plus sensibles d'une personne.

En conséquence, la Commission est d'avis que tout ce qui entoure l'usage de la biométrie devrait faire partie du projet de loi. La loi devrait clairement établir que le recours à la biométrie doit être limité pour des fins d'identification et d'authentification. Elle devrait aussi prévoir comment ces renseignements seront protégés et que leur utilisation doit se limiter qu'aux situations où d'autres moyens moins intrusifs ne permettent pas d'atteindre l'objectif poursuivit. À tout le moins, le projet de loi devrait prévoir que l'usage de la biométrie ne peut jamais être imposé et que des moyens alternatifs doivent être prévus. De l'avis de la Commission, tout usage de la biométrie doit être prévu au projet de loi pour que cet usage puisse faire l'objet d'un débat public afin d'assurer le plus haut niveau de transparence concernant la collecte et l'utilisation de ces renseignements sensibles.

Par ailleurs, la Commission souligne que le critère de nécessité devra être respecté pour toute utilisation de la biométrie dans le cadre de l'IN nationale puisque les règles en matière de protection des renseignements personnels ainsi que la LCCJTI s'appliquent. De plus, l'utilisation de la biométrie devra également faire l'objet d'une divulgation préalable à la Commission ainsi que d'un consentement exprès de la personne concernée[55].

Recommandation 17 : la Commission recommande :

- **De retirer du projet de loi le pouvoir réglementaire résiduaire du gouvernement prévu au paragraphe 4° de l'article 10.9 de la LMCN, tel qu'édicté par l'article 6 du projet de loi;**
- **Prévoir, directement dans le projet de loi, tout l'encadrement relatif à l'usage de la biométrie dans le cadre de l'IN nationale.**

2.3.8. Autres commentaires

Le décret numéro 1084-2024 et le pouvoir habilitant prévu par l'article 10.5 de la LMCN

L'article 38 du projet de loi prévoit que le décret numéro 1084-2024 du 10 juillet 2024 est réputé pris en vertu du deuxième alinéa de l'article 10.5 de la LMCN[56]. Le pouvoir habilitant prévu au deuxième alinéa de l'article 10.5 permet au gouvernement de soustraire un organisme public de l'obligation de recourir aux services du ministre relatifs à l'IN nationale[57]. Or, concrètement, le décret 1084-2024 du 10 juillet 2024 ne soustrait aucun organisme de l'obligation d'utiliser un service du ministre. Il prévoit plutôt :

[54] Article 10.9 al. 1 par. 3 de la LMCN, édicté par l'article 6 du projet de loi.
[55] LCCJTI, précité note 3, article 44.
[56] Article 10.5 de la LMCN, édicté par l'article 6 du projet de loi.
[57] Article 10.5 al. 1 de la LMCN, édicté par l'article 6 du projet de loi.

- Que tous les organismes visés à l'article 2 de la LGGRI sont tenus d'utiliser le Service d'authentification gouvernementale du ministre au plus tard le 31 mars 2028 pour chacune de leurs prestations électroniques de services et;
- Que les organismes publics qui utilisent déjà un autre service d'authentification des personnes pour une prestation électronique de services doivent continuer d'utiliser ce service jusqu'au rattachement de cette prestation au Service d'authentification gouvernementale du ministre au plus tard le 31 mars 2028.

Bref, la Commission se questionne à savoir quel organisme est soustrait de l'obligation d'utiliser les services du ministre dans ce décret. Celui-ci semble plutôt porter sur des modalités de rattachement des organismes publics au Service d'authentification gouvernemental.

Le pouvoir de transférer toute fonction ou une partie d'une fonction d'un organisme public à un autre

Le pouvoir habilitant du gouvernement prévu au deuxième alinéa de l'article 10.6 de la LMCN permet notamment au gouvernement de confier à un organisme public toute fonction ou transférer une partie d'une fonction d'un organisme public à un autre.

La Commission souhaite souligner que la possibilité pour le gouvernement de confier à un organisme public toute fonction ou transférer une partie d'une fonction d'un organisme public à un autre est une nouvelle possibilité qui n'existe pas dans le régime de la source officielle de données gouvernementale comme prévu par la LGGRI. Cet ajout permet au gouvernement de transférer une fonction d'un organisme public prévu législativement par simple décret. La Commission se questionne sur l'opportunité de cette habilitation législative et souligne que celle-ci peut avoir un impact en matière de protection des renseignements personnels. En effet, la nécessité pour un organisme public de recueillir, d'utiliser et de communiquer des renseignements s'évalue notamment à la lumière des fonctions de cet organisme. Entre autres, un tel transfert des fonctions d'un organisme public à un autre peut avoir comme conséquence la collecte, l'utilisation et la communication de renseignements personnels entre organismes publics sans le consentement des personnes concernées et pour des fins différentes que celles prévues à l'origine. Il s'agit d'une mesure du projet de loi qui peut avoir comme conséquence de modifier les règles relatives à l'utilisation des renseignements personnels prévues à la Loi sur l'accès, de restreindre le contrôle des citoyens sur leurs renseignements personnels et qui diminue la transparence relative à la circulation de ces renseignements entre les organismes.

3. Les autres dispositions du projet de loi nº 82

Outre les dispositions relatives à l'IN nationale qui sont ajoutées à la LMCN, le projet de loi prévoit d'autres modifications à cette loi ainsi qu'à plusieurs autres lois ou règlements. Dans la présente section, la Commission souhaite commenter les modifications apportées à LMCN qui ne concernent pas l'IN nationale et certains enjeux liés aux modifications apportées à trois de ces lois, soit : la LAM, la LGGRI et la LAF.

3.1. Les autres modifications apportées à la LMCN

Les articles 1 à 5 du projet de loi modifient la LMCN. En bref, ces modifications portent essentiellement sur les fonctions du ministre de la Cybersécurité et du Numérique :

- L'élargissement des services que le ministre peut offrir, puisque ces services pourraient porter sur des services en ressources informationnelles[58] (plutôt qu'à des services plus spécifiques en matière d'infrastructures technologiques et en systèmes de soutien communs);
- L'ajout d'une fonction spécifique concernant les infrastructures et les services de télécommunications ainsi que sur la mise en place d'un réseau d'infrastructures de connectivité en lien avec les services de télécommunications fournis[59];
- L'ajout d'une fonction à titre de courtier en technologies spécialisées[60];

[58] Modification des articles 4 et 5(1º) de la LMCN, telle que modifiée par les articles 1 et 2 du projet de loi. Le Grand dictionnaire terminologique de l'Office québécois de la langue française définit ainsi les termes ressources informationnelles : « Ensemble des ressources utilisées par une organisation, dans le cadre de ses activités de gestion de l'information, pour l'accomplissement de sa mission, pour la prise de décision ou pour la résolution de problèmes. Les ressources informationnelles incluent notamment les ressources humaines, matérielles, financières ou technologiques directement affectées à l'acquisition, au développement, à l'entretien, à l'exploitation, au traitement, à la circulation, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information. Une personne, un fichier ou un système informatique, par exemple, peut faire partie des ressources informationnelles d'une organisation. », en ligne : <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8364533/ressources-informationnelles>.

[59] Ajout des articles 5.2 et 5.3 à la LMCN, édicté par l'article 3 du projet de loi.

[60] Modification de l'article 6 de la LMCN, édicté l'article 4 du projet de loi. Le projet de loi ajoute une définition de « technologies spécialisées », s'agissant de biens ou de services technologies relatifs aux progiciels de gestion intégrée, à la cybersécurité, aux fondations servant d'infrastructures technologiques ainsi qu'aux systèmes patrimoniaux de la plateforme applicative sur ordinateur central.

- La possibilité pour le ministre de déterminer lui-même à quelles personnes ou à quelles entités, autres que les organismes publics, il peut fournir les services visés aux articles 4[61], 5.1[62], 5.2[63] et 10.5[64] ainsi que les offres prévues à l'article 6[65].

Considérant que les nouvelles fonctions du ministre sont relativement étendues et qu'elles seront susceptibles d'impliquer régulièrement des renseignements personnels, dont parfois des renseignements sensibles, la Commission souhaite sensibiliser le ministre sur l'importance de considérer et de prévoir la protection des renseignements personnels dès la conception de ses services. Une telle approche en matière de conception de services et de produits technologiques permet d'assurer le respect du cadre législatif applicable et de limiter les risques d'incidents de confidentialité.

Notamment, la confection d'évaluations des facteurs relatifs à la vie privée[66] est un excellent moyen d'inclure la protection des renseignements personnels dès la conception d'un service ou d'un produit technologique. À cet égard, la Commission rappelle que l'évaluation des facteurs relatifs à la vie privée doit démontrer qu'un renseignement personnel bénéficiera d'une protection adéquate, notamment au regard des principes généralement reconnus, lorsqu'il est susceptible d'être communiqué à l'extérieur du Québec[67].

3.2. La LAM

3.2.1. La source officielle de données numériques gouvernementales

Les modifications introduites par le projet de loi à la LAM[68] sont en lien avec la mécanique de la source officielle précédemment présentée. La Commission souligne à nouveau être favorable à ce que l'identification de la source officielle pour la constitution du registre de l'IN nationale ainsi que les données nécessaires à cette fonction soient directement prévues à la loi plutôt que prévues par décret en vertu de la LGGRI. En effet, toute modification subséquente devra être réalisée par voie législative plutôt que par décret. Cela permet un suivi plus rigoureux de telles modifications.

3.2.2. Certaines incohérences

La Commission souhaite soulever que les articles de la LAM modifiés par le projet de loi ont été modifiés ou abrogés par la *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*[69].

[61] Services en ressources informationnelles.
[62] Services de certification, incluant les services de répertoire y afférent, ainsi que les services de signature électronique.
[63] Services de télécommunications.
[64] Services relatifs à l'identité numérique nationale.
[65] Offres infonuagiques et en technologies spécialisées.
[66] Loi sur l'accès, précité, note 18, article 63.5.
[67] *Ibid*., article 70.
[68] Articles 20 et 21 du projet de loi.
[69] L.Q., 2023, c. 5.

3.3. La LGGRI

Le projet de loi modifie quelques dispositions de la LGGRI et la Commission souhaite particulièrement attirer l'attention des parlementaires sur trois modifications qui soulèvent des enjeux importants.

3.3.1. La notion de « préjudice sérieux » - Un risque de confusion

L'article 11 du projet de loi ajoute l'article 12.5.3 à la LGGRI. L'alinéa 1 de cette disposition oblige un organisme public à aviser le ministre de la Cybersécurité et du Numérique lorsqu'il constate qu'une ressource informationnelle ou une information sous sa responsabilité fait l'objet d'une atteinte à sa confidentialité, à sa disponibilité ou à son intégrité et que cette atteinte présente un risque qu'un préjudice sérieux soit causé. L'alinéa 2 de cet article prévoit que le ministre peut, par règlement, « déterminer les cas et les circonstances dans lesquels une atteinte présente un risque de préjudice sérieux ou les critères permettant de déterminer si une atteinte présente un tel risque ».

La Commission voit d'un bon œil que le gouvernement soit informé des incidents relatifs aux ressources informationnelles ou aux informations sous la responsabilité des organismes publics. Il est également souhaitable que cette obligation puisse être étendue aux organisations privées qui détiennent ou exploitent des systèmes ou des infrastructures essentiels[70].

Cependant, la Commission souhaite rappeler que les trois lois-cadres concernant la protection des renseignements personnels dont elle est responsable de surveiller l'application[71] prévoient déjà l'obligation pour les organismes publics et les organisations privées d'aviser la Commission ou, selon le cas, le ministre de la Santé et des Services sociaux et la Commission, lorsqu'un incident de confidentialité impliquant des renseignements personnels présente un risque qu'un préjudice sérieux soit causé. Ces lois prévoient également que les critères à considérer pour l'évaluation du risque qu'un préjudice soit causé à une personne relativement à un incident de confidentialité sont notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables[72]. Elles prévoient également l'obligation que le responsable de la protection des renseignements personnels soit consulté lors de cette évaluation.

La Commission souhaite sensibiliser les parlementaires sur la confusion qui pourrait être créée par la présence dans la législation de deux concepts similaires portant sur des matières intrinsèquement reliées entre elles, mais pouvant mener à des obligations de déclaration différentes. Cela sera d'autant plus vrai si les « cas et les circonstances dans lesquels une atteinte présente un risque de préjudice sérieux ou les critères permettant de déterminer si une atteinte présente un tel risque » qui seraient déterminés dans un règlement du ministre ne sont pas établis avec précaution et en cohérence avec le concept de préjudice sérieux prévu aux trois lois-cadres en matière de protection des renseignements personnels.

[70] Ajout d'un troisième alinéa à l'article 5 de la LGGRI, édicté l'article 7 du projet de loi.
[71] Voir Loi sur l'accès, précité, note 18, article 63.8; Loi sur le privé, précité, note 36, article 3.5; LRSSS, précité note 48, article 108; *Loi sur la gouvernance du système de santé et de services sociaux*, RLRQ, c. G-1.021, article 79, ci-après, la LGSSS.
[72] Loi sur l'accès, précité, note 18, article 63.10; Loi sur le privé, précité, note 36, article 3.7; LRSSS, précité note 48, article 109; LGSSS, précité, note 71, article 80.

Pour aider à prévenir l'incohérence et dans un but de clarté, la Commission est d'avis qu'il serait préférable de prévoir à l'article 12.5.3 de la LGGRI, tel qu'introduit par l'article 11 du projet de loi, que parmi les critères à être déterminés par le ministre pour l'évaluation du risque qu'un préjudice soit causé à une personne lors d'une atteinte se trouvent notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

Finalement, elle souhaite également attirer l'attention des parlementaires sur le fait que les lois-cadres précitées prévoient un pouvoir réglementaire du gouvernement pour « déterminer le contenu et les modalités des avis » devant être faits à la Commission alors que le projet de loi du ministre est muet à cet égard.

Recommandation 18 : la Commission recommande de prévoir à l'article 12.5.3 de la LGGRI, tel qu'introduit par l'article 11 du projet de loi, que parmi les critères à être déterminés par le ministre pour l'évaluation du risque qu'un préjudice soit causé à une personne lors d'une atteinte se trouvent notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

3.3.2. Les modifications aux deuxième et troisième alinéas de l'article 12.14, une diminution importante du contrôle des citoyens sur leurs renseignements et de la transparence

La version actuelle de l'article 12.14 de la LGGRI permet au gouvernement de désigner, par décret, un organisme public à titre de source officielle de données numériques gouvernementales. Également, il permet au gouvernement d'identifier les organismes publics qui devront recueillir des données auprès de la source officielle et les utiliser ou les communiquer à celle-ci. La modification proposée par le ministre à cet article ferait en sorte que les organismes publics seraient automatiquement obligés de recueillir les données numériques gouvernementales auprès d'une source officielle désignée à moins d'en être exemptés par décret du gouvernement. Le ministre souhaite donc renverser complètement la règle actuelle.

Lorsque des renseignements personnels sont concernés, la version actuelle de l'article 12.14 de la LGGRI constitue déjà un régime d'exception à la législation applicable, à la notion du consentement ainsi qu'aux contrôles des citoyens sur leurs renseignements. En effet, dans sa mouture actuelle, la LGGRI prévoit un régime qui permet la collecte, la communication et l'utilisation de renseignements personnels dans des situations qui ne sont pas d'emblée autorisées par la législation applicable. En plus, il s'agit d'une finalité différente de celle à laquelle les citoyens ont consenti. Dans son mémoire[73] déposé publiquement concernant le projet de loi 95, la Commission avait d'ailleurs affirmé que la portée du régime d'exception proposé était trop étendue et risquait de réduire de manière significative la protection accordée aux renseignements personnels et les droits des citoyens prévus par la Loi sur l'accès.

[73] COMMISSION D'ACCÈS À L'INFORMATION, *Projet de loi n°95, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives – Mémoire de la Commission d'accès à l'information présenté à la Commission des finances publiques dans le cadre des consultations particulières et auditions publiques*, 21 mai 2021, en ligne : <https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PL-95.pdf>.

En ce sens, la modification proposée à l'article 12.14 constitue une brèche encore plus significative à la législation actuelle applicable en matière de protection des renseignements personnels. Une telle situation mène à une circulation des renseignements personnels des citoyens de manière opaque et elle dispense les organismes publics de faire le moindre effort pour obtenir le consentement des citoyens. La Commission rappelle que le consentement est l'une des façons pour le citoyen d'assurer le contrôle de ses renseignements personnels. En ce sens, dans tous les cas où un service est initié à la demande d'un citoyen, l'organisme public peut lui demander un consentement afin de recueillir des renseignements personnels d'un autre organisme.

La Commission rappelle également que le projet de loi introduit à la LMCN la fonction spécifique de source officielle en matière d'IN (identification et authentification) et que l'obligation pour les organismes publics d'y recourir s'y trouve spécifiquement. La Commission doute fortement qu'il soit nécessaire que le régime général de source officielle prévoie d'emblée l'obligation pour tous les organismes publics d'y recourir, sans même savoir sur quelles données portera ladite fonction.

La Commission s'oppose donc vivement aux modifications législatives des deuxième et troisième alinéas de l'article 12.14 de la LGGRI, sauf quant à celle portant sur la qualité des données. Le régime actuel de la source officielle de données numériques gouvernementales est déjà un régime d'exception étendu au régime législatif applicable. Les modifications proposées ne font qu'étendre encore plus ce régime d'exception et la Commission est d'avis que rien ne le justifie.

Recommandation 19 : la Commission recommande que la proposition de modification des deuxième et troisième alinéas de l'article 12.14 de la LGGRI, sauf pour le sujet de la qualité des données, soit retirée du projet de loi.

3.3.3. Le retrait du cinquième alinéa de l'article 12.14, l'élimination d'un rempart à l'utilisation de renseignements sensibles des citoyens

Le premier alinéa de l'article 12.14 de la LGGRI prévoit que la désignation d'une source officielle se fait sur recommandation conjointe du ministre de la Cybersécurité et du Numérique et du ministre responsable de l'organisme public qui détient les données numériques gouvernementales concernées.

Il existe cependant une exception à cette règle générale, prévue au 5e alinéa du même article, concernant les renseignements de santé et de services sociaux. En effet, lorsque des données numériques gouvernementales concernées par la mécanique de source officielle envisagée sont détenues par le ministre de la Santé et des Services sociaux ou par tout organisme public relevant de son portefeuille, la désignation de la source officielle de données numériques gouvernementales en application du présent article se fait sur recommandation de ce ministre uniquement et non pas sur recommandation commune de celui-ci et du ministre de la Cybersécurité et du Numérique.

Dans ce contexte, la modification législative proposant de retirer le cinquième alinéa de l'article 12.14 de la LGGRI a pour effet essentiel d'éliminer un rempart à la protection des renseignements parmi les plus sensibles des citoyens en retirant la prérogative du ministre de la Santé et des Services sociaux d'être le seul pouvant recommander la prise d'un tel décret. Tous

les renseignements de santé et de services sociaux pourraient ainsi être utilisés à des fins autres que la santé et les services sociaux des citoyens sans que le ministre responsable de ces renseignements initie lui-même la démarche.

La Commission est d'avis que la prérogative prévue au cinquième alinéa de l'article 12.14 de la LGGRI, qui constitue une mesure de protection des renseignements de santé et de services sociaux, doit être conservée.

Recommandation 20 : la Commission recommande de retirer du projet de loi l'abrogation du cinquième alinéa de l'article 12.14 de la LGGRI.

3.4. La LAF

La Commission souhaite porter deux modifications introduites par le projet de loi à la LAF à l'attention des parlementaires.

3.4.1. La communication sans consentement de renseignements fiscaux

Tout d'abord, l'article 17 du projet de loi prévoit un ajout à l'article 69.1 de la LAF. En vertu de celui-ci, un renseignement contenu dans un dossier fiscal peut être communiqué, sans le consentement de la personne concernée, au ministre de la Cybersécurité et du Numérique, mais uniquement dans la mesure où le renseignement est nécessaire aux fins prévues au chapitre I.1 de la LMCN, soit le chapitre portant sur l'IN.

Cette modification semble liée à l'inscription souhaitée dans la LMCN de la mécanique relative à la source officielle de données numériques gouvernementales aux fins du registre de l'IN. La Commission s'interroge sur les raisons qui justifient cet ajout à la LAF.

En effet, la Commission se questionne sur les renseignements fiscaux précis qui sont nécessaires pour les besoins spécifiques de l'IN nationale et qui feraient l'objet de communication, **sans consentement,** aux fins d'identification ou d'authentification en lien avec l'IN nationale. La Commission constate que dans le décret 870-2022, seules les données de la RAMQ sont communiquées au ministre de la Cybersécurité et du Numérique.

En plus, ce décret prévoit que les données numériques gouvernementales détenues par des organismes publics et nécessaires aux fins de l'authentification de l'identité des personnes voulant avoir accès aux prestations électroniques de services gouvernementaux seront utilisées et communiquées sur la base du consentement de ces personnes. La Commission ne comprend pas pourquoi les renseignements requis ont changé et pourquoi la communication est effectuée sans consentement. Également, la Commission se questionne en quoi ces renseignements sont nécessaires aux fins du registre de l'IN, alors qu'ils ne l'étaient pas au moment de prendre le décret 870-2022. En somme, quels sont les changements qui sont envisagés pour justifier l'ajout d'une nouvelle possibilité de communication de renseignements personnels sensibles sans le consentement des personnes concernées?

En effet, il semble qu'actuellement cette communication peut être réalisée avec le consentement des personnes concernées. Lorsqu'elle est possible, cette approche est à préconiser puisque le consentement permet aux personnes d'exercer un contrôle sur leurs renseignements

personnels. En matière d'IN, il s'agit d'un élément important pour la mise en place d'une IN bien élaborée. Une telle approche favorise l'adhésion des citoyens aux solutions d'IN. La Commission est d'avis qu'il n'est pas opportun de reproduire cet aspect législatif de la source officielle puisqu'il ne semble pas nécessaire dans le cadre de l'IN nationale d'obtenir des renseignements fiscaux sans le consentement des personnes concernées.

Recommandation 21 : la Commission recommande de retirer l'article 17 du projet de loi.

3.4.2. Le retrait de l'approbation de la Commission relative aux règles encadrant la gouvernance

L'article 18 du projet de loi prévoit plusieurs modifications à l'article 69.1.1 de la LAF. L'une de celles-ci est le remplacement de l'approbation des règles encadrant la gouvernance de renseignements par la Commission par une simple transmission à cette dernière. Cette modification pourrait sembler en être une de concordance avec la LGGRI. En effet, lorsque le régime de la LGGRI a été modifié[74], l'approbation par la Commission des règles de gouvernance prévue au paragraphe 2° du premier alinéa de l'article 12.16 de la LGGRI a été remplacée par une transmission à celle-ci.

Cependant, lorsque cette modification a été introduite, l'approbation des règles de gouvernance par la Commission dans la LAF a été maintenue. De l'avis de la Commission, ce choix du législateur peut notamment s'expliquer parce que les renseignements visés à la LAF sont des renseignements sensibles et qu'il était essentiel que des mesures de protection accrues leur soient applicables. La Commission est d'avis que cette approbation doit être maintenue en raison de la protection accrue dont les renseignements fiscaux doivent bénéficier, tel que le législateur l'a initialement souhaité.

Recommandation 22 : la Commission recommande de retirer la modification du projet de loi qui prévoit que les règles de gouvernance lui sont transmises et de maintenir son approbation à l'égard de celles-ci.

[74] *Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives*, L.Q. 2023, c. 28.

4. Conclusion

La Commission reconnaît l'importance du travail effectué en matière d'IN au cours des dernières années et ayant mené au dépôt du projet de loi par le ministre.

Toutefois, et tel qu'exposé dans ce mémoire, elle constate que plusieurs éléments du projet de loi devraient être bonifiés afin de permettre la réalisation des objectifs légitimes de celui-ci, tout en s'assurant du respect des droits des citoyens.

Bien qu'elle comprenne que le présent projet de loi tende vers une neutralité technologique, la Commission déplore le fait que le projet de loi en dise aussi peu sur le fonctionnement réel de l'IN nationale et qu'une part importante de celle-ci soit déférée au pouvoir réglementaire du ministre. D'une part, cette approche empêche une compréhension globale du projet d'IN nationale parce qu'elle ne permet pas une vue d'ensemble. D'autre part, cette approche n'offre pas les mêmes garanties de transparence que le processus législatif.

D'ailleurs, l'expérience d'autres juridictions en matière d'IN démontre l'importance d'introduire un cadre législatif complet et transparent, qui permet aux citoyens une compréhension globale du fonctionnement de l'IN. Une telle compréhension du fonctionnement de l'IN ne peut que favoriser l'adhésion des citoyens à l'IN nationale au Québec.

En somme, la Commission souhaite souligner l'importance de trouver le niveau d'équilibre entre la souplesse que requiert un projet technologique de cette ampleur et la nécessité d'avoir une vision globale claire. Un tel équilibre permettra d'instaurer l'IN nationale au Québec avec les plus hauts standards en matière de protection des renseignements personnels, dans un cadre transparent qui permet les débats sociaux et la consultation de la population.

Liste des recommandations

Recommandation 1 : la Commission estime que la définition de l'IN nationale doit être clarifiée et que les termes utilisés dans le chapitre I.1 de la LMCN ne doivent pas susciter d'ambiguïté avec les termes utilisés dans les autres documents relatifs à l'IN nationale, comme les Règles relatives à l'assurance de l'identité numérique.

Recommandation 02 : la Commission recommande de décrire au projet de loi les acteurs du triangle de confiance, soit le détenteur, l'émetteur et le vérificateur.

Recommandation 03 : la Commission recommande que le projet de loi interdise au ministre et à toute organisation publique ou privée d'utiliser les données contenues au registre de l'IN nationale à une fin autre que celles nécessaires à l'exercice des fonctions prévues au chapitre I.1 de la LMCN;

Recommandation 04 : la Commission recommande :

- **Que le projet de loi prévoie que la vérification d'une attestation ne doit permettre que la divulgation minimale de renseignements personnels selon le contexte de la vérification effectuée. Au surplus, toute modalité requise à cet égard devrait être prévue par voie réglementaire (cadre de confiance);**
- **Que le projet de loi oblige l'obtention d'un consentement exprès du détenteur d'une attestation et qu'il permette à celui-ci, dans les cas où cela est possible, de déterminer l'attestation à présenter. Toutes les modalités relatives au consentement devraient être prévues par les règlements du ministre.**

Recommandation 05 : la Commission recommande l'ajout de recours pour les citoyens au projet de loi.

Recommandation 06 : la Commission recommande l'ajout de sanctions pour la contravention du cadre normatif de l'IN nationale. Plus spécifiquement, la Commission suggère d'ajouter une infraction correspondant au non-respect des obligations imposées aux différents acteurs de l'écosystème de l'IN.

Recommandation 07 : la Commission recommande

- **D'ajouter une interdiction pour les organisations privées et les organismes publics d'effectuer du profilage, du traçage ou de la surveillance à l'aide de l'IN nationale ou des renseignements qui découlent de son utilisation et que le non-respect de cette interdiction constitue une infraction.**
- **Que le projet de loi contienne des restrictions claires et précises concernant l'interdiction de tracer ou surveiller les citoyens eux-mêmes, mais également les transactions effectuées par les citoyens à l'aide de l'IN ou d'effectuer des activités de géolocalisation avec ces mêmes données.**

Recommandation 08 : la Commission recommande que le projet de loi identifie les normes opérationnelles minimales requises avant le déploiement de l'IN nationale dans les organismes publics, afin que le ministre adopte les règles conséquentes à ces normes minimales.

Recommandation 09 : la Commission recommande d'ajouter au projet de loi une obligation de révision périodique, laquelle pourrait inclure une consultation publique.

Recommandation 10 : la Commission recommande qu'un organisme indépendant soit désigné afin de surveillance l'application du chapitre I.1 de la LMCN.

Recommandation 11 : la Commission recommande de prévoir au projet de loi que le gouvernement doit prévoir les conditions et modalités relatives aux ententes des organismes publics pour l'interopérabilité de l'IN nationale.

Recommandation 12 : la Commission recommande qu'un droit d'accès à un registre des transactions soit prévu au projet de loi.

Recommandation 13 : la Commission recommande que l'imposition de l'IN nationale soit interdite en tout temps. De plus, l'article 10.3 du projet de loi devrait prévoir que les organismes publics doivent offrir d'autres moyens d'identification raisonnablement pratiques et accessibles.

Recommandation 14 : la Commission recommande d'expliquer davantage le concept de contrôle des citoyens et de prévoir au projet de loi que le consentement doit être exprès et qu'il peut être retiré en tout temps.

Recommandation 15 : la Commission recommande d'ajouter au projet de loi une obligation du ministre d'informer la population, notamment quant aux risques liés à l'utilisation de l'IN nationale et aux mesures à prendre pour en assurer la protection.

Recommandation 16 : la Commission recommande :

- **Que toutes les données numériques gouvernementales connues soient identifiées directement au projet de loi plutôt que par référence au décret 870-2022 du 25 mai 2022;**
- **Que le contenu du registre de l'IN nationale soit prévu au chapitre I.1 de la Loi;**
- **Qu'une disposition équivalente à l'article 12.11 de la LGGRI soit ajoutée au projet de loi.**

Recommandation 17 : la Commission recommande :

- **De retirer du projet de loi le pouvoir réglementaire résiduaire du gouvernement prévu au paragraphe 4o de l'article 10.9 de la LMCN, tel qu'édicté par l'article 6 du projet de loi;**
- **Prévoir, directement dans le projet de loi, tout l'encadrement relatif à l'usage de la biométrie dans le cadre de l'IN nationale.**

Recommandation 18 : la Commission recommande de prévoir à l'article 12.5.3 de la LGGRI, tel qu'introduit par l'article 11 du projet de loi, que parmi les critères à être déterminés par le ministre pour l'évaluation du risque qu'un préjudice soit causé à une personne lors d'une atteinte se trouvent notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

Recommandation 19 : la Commission recommande que la proposition de modification des deuxième et troisième alinéas de l'article 12.14 de la LGGRI, sauf pour le sujet de la qualité des données, soit retirée du projet de loi.

Recommandation 20 : la Commission recommande de retirer du projet de loi l'abrogation du cinquième alinéa de l'article 12.14 de la LGGRI.

Recommandation 21 : la Commission recommande de retirer l'article 17 du projet de loi.

Recommandation 22 : la Commission recommande de retirer la modification du projet de loi qui prévoit que les règles de gouvernance lui sont transmises et de maintenir son approbation à l'égard de celles-ci.

Québec
525, boul. René-Lévesque Est
Bureau 2.36
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741

Montréal
2045, rue Stanley
Bureau 900
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196

CAI Commission d'accès à l'information du Québec

1 888 528-7741 | cai.gouv.qc.ca