PROJET DE LOI 82

LOI CONCERNANT L'IDENTITÉ NUMÉRIQUE NATIONALE ET MODIFIANT D'AUTRES DISPOSITIONS

MÉMOIRE

À LA COMMISSION DES FINANCES PUBLIQUES

ASSEMBLÉE NATIONALE DU QUÉBEC

24 JANVIER 2025

Table des matières

Présentation de la Ligue des droits et libertés

Fondée en 1963, la Ligue des droits et libertés (LDL) est un organisme à but non lucratif, indépendant et non partisan, qui vise à faire connaître, à défendre et à promouvoir l'universalité, l'indivisibilité et l'interdépendance des droits reconnus dans la Charte internationale des droits de l'Homme. La Ligue des droits et libertés est affiliée à la Fédération internationale pour les droits humains (FIDH).

La LDL poursuit, comme elle l'a fait tout au long de son histoire, différentes luttes contre la discrimination et contre toute forme d'abus de pouvoir, pour la défense des droits civils, politiques, économiques, sociaux et culturels. Son action a influencé plusieurs politiques publiques et a contribué à la création d'institutions vouées à la défense et à la promotion des droits humains, notamment l'adoption de la Charte des droits et libertés de la personne du Québec et la création de la Commission des droits de la personne et des droits de la jeunesse.

Elle interpelle, tant sur la scène nationale qu'internationale, les instances gouvernementales pour qu'elles adoptent des lois, mesures et politiques conformes à leurs engagements à l'égard des instruments internationaux de défense des droits humains et pour dénoncer des situations de violation de droits dont elles sont responsables. La LDL mène des activités d'information, de formation, de sensibilisation visant à faire connaître le plus largement possible les enjeux de droits pouvant se rapporter à l'ensemble des aspects de la vie en société. Ces actions visent l'ensemble de la population, de même que certains groupes placés, selon différents contextes, en situation de discrimination.

Nous remercions la Commission des finances publiques de cette invitation à participer aux consultations particulières et auditions publiques sur le projet de loi 82, *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions*.

Introduction

Depuis des années, la LDL s'intéresse à la protection des renseignements personnels, élément essentiel du droit à la vie privée et du respect des droits humains. Nous avons soumis des mémoires dans le cadre des consultations sur le projet de loi nº 64 (*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Loi 25), sur le projet de loi nº 3 (*Loi sur les renseignements de santé et de services sociaux*, Loi 5) et sur le projet de loi nº 38 (*Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*). Le projet de loi nº 82 (PL 82), instaurant les fondements de l'identité numérique nationale (INN), soulève lui aussi plusieurs enjeux de vie privée et d'autres droits humains.

Nous regrettons que ce projet de loi intervienne à un stade si avancé du programme d'identité numérique, pourtant en cours depuis au moins 2021. Le mémoire au Conseil des ministres[1], visant l'autorisation du projet, indique que divers ministères et organismes publics ont été consultés dans son élaboration, de même que des gens d'affaires.

Mais encore bien peu de détails ont été divulgués sur le fonctionnement technique du système et son mode de gouvernance ; et aucun débat public n'a permis de discuter des choix faits par le gouvernement et des besoins de la population. À cet égard, la démarche ne rencontre pas, selon nous, les prescriptions de transparence établies par les commissaires à la vie privée du pays dans l'établissement d'une identité numérique[2]. À cet égard, la Commission d'accès à l'information (CAI), précisait dans un communiqué du 24 octobre 2022 :

> « Le gouvernement doit faire preuve de transparence à toutes les étapes de la réalisation du projet d'identité numérique en sollicitant la participation citoyenne, à travers des consultations élargies, comme l'ont fait certaines provinces[3] ».

Quant au PL 82, il nous en apprend peu sur les tenants et aboutissants du système et semble surtout destiné à pérenniser plusieurs éléments déjà instaurés par décrets (registre, source officielle de données, obligation pour les organismes publics d'utiliser le Service d'authentification

---

[1] Gouvernement du Québec, *Autorisation de la phase d'exécution du projet Identité numérique citoyenne découlant du Programme Service québécois d'identité numérique*, Mémoire au Conseil des ministres (partie accessible au public), 8 décembre 2021. En ligne : https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/2021-0227_memoire.pdf

[2] Commissariat à la protection de la vie privée du Canada, *Assurer le droit à la vie privée et la transparence dans l'écosystème d'identité numérique au Canada*, Résolution des commissaires à la protection de la vie privée fédéral, provinciaux et territoriaux et des ombudsmans qui assument une fonction de surveillance dans le domaine, 21 septembre 2022. 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-territoires/res_220921_02/

> « Les commissaires à la protection de la vie privée du Canada et les ombudsmans qui assument une fonction de surveillance dans le domaine au pays demandent à leurs gouvernements respectifs et aux intervenants concernés de **veiller à ce que le droit à la vie privée et le principe de transparence soient pleinement respectés tout au long de la conception, de l'exploitation et de l'évolution de l'écosystème d'identité numérique au Canada** ».

[3] Commission d'accès à l'information. *Identité numérique au Canada : les organismes de surveillance demandent aux gouvernements d'assurer le droit à la vie privée et la transparence dans leurs projets et systèmes*, Communiqué de presse, 24 octobre 2022. En ligne : https://www.quebec.ca/nouvelles/actualites/details/identite-numerique-au-canada-les-organismes-de-surveillance-demandent-aux-gouvernements-dassurer-le-droit-a-la-vie-privee-et-la-transparence-dans-leurs-projets-et-systemes-43613

gouvernementale) ; tout cela sans débat[4]. Si nous saluons l'adoption d'un encadrement légal pour l'INN, celui qui est proposé ici soulève plusieurs inquiétudes.

Nous limiterons nos commentaires aux dispositions[5] sur l'identité numérique relatives (1) à la gestion centralisée de l'INN ; (2) à l'interdiction de profilage ; (3) à l'utilisation de la biométrie ; (4) à la fracture numérique ; (5) au portefeuille numérique ; (6) aux pouvoirs règlementaires et (7) à l'interopérabilité.

1. Identité numérique nationale (INN) : une gestion centralisée

Le PL 82 confie au ministre de la Cybersécurité et du Numérique (le ministre) la gestion centralisée de l'INN (cadre de gouvernance, cohérence et qualité des renseignements). À cette fin, la *Loi sur le ministère de la Cybersécurité et du Numérique* (LMCN) s'enrichit d'un chapitre I.1 intitulé *Identité numérique nationale* (les articles 10.2 à 10.10)[6].

L'INN est par ailleurs décrite comme l'ensemble des moyens dont dispose l'État pour permettre :

- un accès sécurisé aux prestations électroniques de services gouvernementales ;
- un niveau de confiance élevé lors d'interactions avec les organismes publics et dans la collectivité, à l'aide d'attestations numériques gouvernementales[7].

Le ministre agira comme source officielle de données numériques gouvernementales (DNG) pour les besoins de l'INN. Les DNG comprennent :

- le nom et les date et lieu de naissance d'une personne physique ainsi que le nom de ses parents ;
- le nom et les coordonnées d'une personne morale ou d'une société de personnes ;
- tout autre renseignement que détermine le gouvernement[8].

Est aussi institué le registre de l'INN (RINN), soit un système de dépôt et de communication des DNG sous responsabilité du ministre. Le RINN doit permettre :

- 1° la conservation sécuritaire, pour le compte d'un organisme public, de tout ou partie de ces données ;
- 2° la communication entre organismes publics de ces données ;
- 3° l'accès à ces données ;

---

[4] Gouvernement du Québec, *Projet de loi concernant l'identité numérique nationale et modifiant d'autres Dispositions*, Mémoire au Conseil des ministres (partie accessible au public), novembre 2024. En ligne : https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/24-25/2024-0179_memoire.pdf

> Le mémoire indique d'ailleurs : « Bien que les travaux concernant l'identité numérique aient progressé depuis que certains des projets qui composent le Programme SQIN sont en exécution, aucun organisme public n'est désigné responsable de son encadrement au Québec. En effet, les fonctions, les pouvoirs, les responsabilités, les devoirs et les obligations en matière d'identité numérique ne sont pas enchâssés législativement. » (p. 3)

[5] Il s'agit essentiellement l'article 6 du PL 82 ajoutant le chapitre I.1 à la *Loi sur le ministère de la Cybersécurité et du Numérique* (LMCN) incluant les articles 10.2 à 10.10.

[6] PL 82, article 6.

[7] Article 10.2.

[8] Article 10.6.

- 4° la traçabilité de tout accès au registre par une personne, que ce soit pour y déposer ces données, les utiliser ou en recevoir la communication ;
- 5° toute autre fonctionnalité déterminée par règlement du ministre[9].

En réalité, ce registre existe déjà : c'est le registre d'attributs d'identité gouvernemental (RAIG), établi par décret le 25 mai 2022, et qui devient le RINN en vertu de l'art. 40 du PL 82[10]. Le RAIG se compose des renseignements suivants :

> 1° le nom ; 2° pour les femmes mariées avant le 2 avril 1981, le nom du mari ; 3° la date de naissance ; 4° la date du décès ; 5° l'adresse de résidence et son historique ; 6° l'indicateur de présence d'un répondant ; 7° le numéro d'assurance maladie ; 8° le numéro d'assurance sociale et son historique ; 9° l'identifiant sectoriel de la Régie de l'assurance maladie du Québec[11].

Ces informations proviennent de la Régie de l'assurance maladie (RAMQ)[12] . Des renseignements fiscaux pourraient aussi être communiqués aux fins de l'INN[13].

À quoi sert ce registre ? Selon ce qu'indique le mémoire soumis au conseil des ministres pour l'adoption du décret sur le RAIG, les données du registre :

> « [...] permettront de rechercher un citoyen dans le registre, de l'identifier en s'assurant qu'il est bien la personne qu'il prétend être, et également de l'authentifier, à la suite de vérification de secrets (une information connue que par le citoyen et l'organisme public détenteur de cette information)[14] ».

Le document ministériel précise aussi que le ministère de la Cybersécurité et du Numérique (MCN) a opté pour un chargement massif et immédiat des attributs d'identités :

> « Bien qu'il aurait été possible de créer le registre d'attributs d'identité au fur et à mesure des demandes d'utilisation du Service d'authentification gouvernementale, le choix retenu s'est plutôt dirigé vers un chargement massif des attributs d'identité détenus par la RAMQ, suivi par des mises à jour fréquentes[15] ».

Bref, de très nombreux renseignements personnels sont inscrits au RAIG qui deviendra le RINN. Une telle centralisation de renseignements personnels comporte des risques importants. Les craintes

---

[9] Article 10.7.

[10] PL 82, article 40. « Le registre d'attributs d'identité gouvernemental visé par le décret numéro 870-2022 du 25 mai 2022 **devient le registre de l'identité numérique nationale** visé à l'article 10.7 de la Loi sur le ministère de la Cybersécurité et du Numérique (chapitre M-17.1.1), édicté par l'article 6 de la présente loi. ».

[11] Gouvernement du Québec*, Décret 870-2022*, 25 mai 2022. En ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2022F/77391.pdf

[12] Idem. Voir aussi l'article 20 du PL 82 modifiant la *Loi sur l'assurance maladie* pour que la RAMQ transmettent au MCN sur demande : les noms, date de naissance, sexe, adresse ou numéros de téléphone d'une personne inscrite à son fichier d'inscription des personnes assurées ainsi que les noms du conjoint d'une telle personne.

[13] PL 82, article 17 modifiant la *Loi sur l'administration fiscale*.

[14] Gouvernement du Québec, *Désignation du ministère de la Cybersécurité et du Numérique pour agir comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale à implanter dans le cadre de la réalisation du projet Accès bonifié aux prestations électroniques de services Citoyens du Programme Service québécois d'identité numérique*, Mémoire au conseil des ministres, p.3. En ligne : https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/2022-1618_memoire.pdf

[15] Idem, p. 5.

sont d'autant plus vives que les règles encadrant la gouvernance de tels renseignements ne nécessitent plus l'approbation de la CAI à la suite de l'adoption du projet de loi nº 38[16].

Il s'agit de données sensibles visant à assurer l'unicité des individus. Le registre englobe les données de pratiquement toute la population du Québec. Il pourrait même inclure des caractéristiques ou mesures biométriques[17]. La résolution commune des Commissaires à la vie privée sur l'identité numérique[18] énonce pourtant que les systèmes d'identification numérique « ne devraient pas créer de bases de données centralisées ».

Une banque centralisée présente des dangers importants comme l'indique ce groupe d'experts français :

> « Dans le cadre d'une architecture centralisée, les identités numériques des citoyens sont gérées dans une base de données centrale et l'association de chaque citoyen à son identité se fait par une authentification à un ou plusieurs facteurs. (…) Ce type d'architecture rend le système plus sensible aux attaques de sécurité : que ces attaques soient liées à un aspect technologique ou à une défaillance humaine. En effet, les systèmes centralisés sont de plus en plus ciblés par les attaques ou les arrêts système (attaques par déni de service)[19] ».

Un registre réunissant autant de renseignements personnels en un seul fichier ne peut qu'attiser la convoitise des cybercriminels et favoriser les actes de piratage[20]. Une fuite de données pourrait aussi résulter de l'action à l'interne d'un employé — comme dans le cas de la fuite massive chez Desjardins [21] ou encore de déficiences de contrôle et de sécurité.

À titre d'exemple, le rapport 2023-2024 de la Vérificatrice générale fait état de graves problèmes dans le contrôle d'accès aux renseignements dans le réseau de santé :

> « Les contrôles de prévention et de détection d'accès non autorisés ne permettent pas aux entités auditées de s'assurer que seuls les utilisateurs dont les fonctions le requièrent accèdent aux renseignements personnels numériques des usagers : Il existe des déficiences dans la gestion des accès aux systèmes audités[22] ».

---

[16] Projet de loi no 38 (2023, chapitre 28), 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*, article 10. En ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2023/2023C28F.PDF

[17] Les pouvoirs règlementaires prévus à l'article 10.9 autoriserait le gouvernement à « 3° 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; »

[18] Commissariat à la protection de la vie privée du Canada, *op cit*., note 2.

[19] INGROUPE, Quels sont les atouts de l'identité numérique décentralisée ? Consultée le 24 janvier 2025. En ligne : https://ingroupe.com/fr/observatoire/atouts-identite-numerique-decentralisee/

[20] Voir le cas du système Aadhar en Inde : Radio-Canada, *Un piratage massif compromet l'identité de 1 milliard d'Indiens*, Radio-Canada, 11 septembre 2018. En ligne : https://ici.radio-canada.ca/nouvelle/1123092/aadhaar-piratage-inde-identite-banque-donnees-empreintes-digitales-iris

[21] Commissariat à la protection de la vie privée du Canada, *Un ensemble de lacunes a donné lieu à la fuite massive de données chez Desjardins*, Communiqué, 14 décembre 2020. En ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/nr-c_201214/

[22] Vérificateur général du Québec, *Protection des renseignements personnels numériques des usagers du réseau de la santé et des services sociaux* – Audit de performance, Rapport à l'Assemblée nationale 2023-2024, novembre 2023, chapitre 3, p.79. En ligne : https://www.vgq.qc.ca/Fichiers/Publications/rapport-annuel/204/VGQ_nov2023_ch3_RenseignementsPerso.pdf

Le MCN n'est pas à l'abri de tels incidents de confidentialité ; un communiqué du MCN émis le 7 août dernier révèle une violation de la confidentialité touchant 3 500 employés de la fonction publique[23].

Un incident de confidentialité (cyberattaque, rançongiciel, fuite, accès interdit, négligence etc.) pourrait entraîner des conséquences désastreuses dans le cas d'un registre concernant des millions de personnes. De même qu'une panne du système informatique pourrait impacter l'ensemble des services gouvernementaux. La panne mondiale causée du 19 juillet 2024 par une mise à jour logicielle de Microsoft démontre la fragilité des systèmes informatiques et la dépendance aux entreprises infonuagiques.

Se pose à cet égard la question de l'endroit où sont stockées les données de l'INN. Le PL 82 n'indique rien à ce sujet. Le stockage hors frontière ou via des entreprises soumises au contrôle de gouvernements étrangers, notamment américain, peut compromettre la souveraineté numérique du Québec sur les données de ses citoyens :

> « Rappelons que depuis 2001, l'US Patriot Act autorise les services de sécurité américains à accéder aux données, détenues par des particuliers ou des entreprises, et stockées sur le territoire américain. De plus, depuis mars 2018, le Cloud Act permet à ces mêmes autorités américaines d'accéder aux données hébergées (en infonuagerie) par un fournisseur américain, même si ces informations sont stockées à l'étranger[24] ».

2. Profilage

L'article 10.7 prévoit que le RINN forme un système de dépôt et de communication des DNG permettant la conservation, la communication, l'accès et la traçabilité des accès au registre. Il ajoute :

> « Le ministre ne peut utiliser **ces données** à des fins de profilage des personnes.
>
> Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'**évaluer certaines caractéristiques d'une personne physique**, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne[25] ».

L'interdit énoncé à l'article 10.7 est ambigu. Que vise-t-on par *ces données* ? Les données du RINN (attributs d'identité) et/ou de ses activités (accès, communication) ? Par ailleurs, l'interdiction concerne uniquement le ministre et ne vise que le profilage, une opération très délimitée dans la mesure où elle consiste à « évaluer certaines caractéristiques d'une personne physique ». Il y a bien

---

[23] Gouvernement du Québec, *Le ministère de la Cybersécurité et du Numérique a pris des mesures immédiates pour protéger les employés de la fonction publique après une violation de la confidentialité*, Communiqué, Ministère de la Cybersécurité et du Numérique, 7 août 2024. En ligne : https://www.quebec.ca/nouvelles/actualites/details/le-ministere-de-la-cybersecurite-et-du-numerique-a-pris-des-mesures-immediates-pour-proteger-les-employes-de-la-fonction-publique-apres-une-violation-de-la-confidentialite-57608

> Le communiqué indique : « […] un employé d'un prestataire de services a transféré, hors des lieux de travail, des documents, dont certains contenaient des renseignements personnels d'employés de la fonction publique. »

[24] Henri-Paul Rousseau, La souveraineté numérique en agroalimentaire au Canada et au Québec, Cirano, 16 février 2021. En ligne : https://cirano.qc.ca/files/publications/2021PE-03.pdf

[25] Article 10.7 (al. 3 et 4) du chapitre I.1 (article 6 du PL 82).

d'autres façons d'utiliser les données : application de la loi, enquête policière, intelligence artificielle, recherche, etc.

Pour la LDL, le système d'INN doit être dédié exclusivement à l'identification et l'authentification des personnes. La loi devrait interdire clairement toute autre utilisation, et ce par quiconque. C'est du reste ce que recommandent les Commissaires à la vie privée dans leur résolution commune :

> « **Les renseignements personnels contenus dans un écosystème d'identité ne devraient pas être utilisés à d'autres fins que l'évaluation et la vérification de l'identité** ou à d'autres fins autorisées qui sont nécessaires pour fournir le service. Les écosystèmes ne devraient pas permettre le suivi ou le traçage de l'utilisation des justificatifs d'identité à d'autres fins[26] ».

3. Biométrie

Le gouvernement s'attribue le pouvoir règlementaire de « préciser les données numériques gouvernementales, ayant des caractéristiques biométriques ou contenant des mesures biométriques, qui peuvent être utilisées » aux fins de l'INN. Le règlement établirait les cas et conditions d'utilisation de telles données.

Le 25 avril 2024, lors de l'étude des crédits du MCN, le ministre indiquait travailler déjà à la mise en place d'une infrastructure reposant sur la biométrie pour l'INN, et ce, avant tout débat public sur la question :

> « Je ne vous cache pas qu'on met en place des infrastructures qui permettraient une identification par biométrie parce que ça nous amène à un niveau de sécurité qui est supérieur. Ceci étant dit, avant d'aller là, il y aura des… il y aura des démarches qui seront entreprises par notre gouvernement, notamment pour s'assurer de l'acceptabilité sociale d'un tel projet. Mais la technologie, si tant est que les Québécois y soient favorables, le permettrait[27] ».

La résolution commune des commissaires à la vie privée sur l'identité numérique ne préconise pas le recours à la biométrie :

> « La collecte ou l'utilisation de renseignements particulièrement intimes, sensibles et permanents, comme les données biométriques, ne devraient être envisagées que s'il est démontré que d'autres moyens moins intrusifs ne permettent pas d'atteindre l'objectif poursuivi[28] ».

Le recours à la biométrie semble en pleine expansion au Québec. En 2023-2024, la CAI a reçu 124 déclarations de banque de caractéristiques biométriques, soit 118 du secteur privé et 6 du secteur public. « Il s'agit d'une augmentation de 59 % par rapport à l'année précédente[29] ».

---

[26] Commissariat à la protection de la vie privée du Canada, *op cit*., note 2.

[27] Assemblée nationale du Québec, Journal des débats de la Commission des finances publiques, Étude des crédits budgétaires du ministère de la Cybersécurité et du Numérique, vol. 47, no 44, 25 avril 2024. En ligne : https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/cfp-43-1/journal-debats/CFP-240425-2.html

[28] Commissariat à la protection de la vie privée du Canada, *op cit*., note 2.

[29] Commission d'accès à l'information, Rapport annuel d'activités et de gestion 2023-2024. En ligne : https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_RAAG_2023-2024.pdf. Voir aussi Charles-Éric Blais-Poulin, *Usage de la*

L'usage de la biométrie semble se répandre aussi au sein du gouvernement québécois. En 2020, la Sûreté du Québec concluait un contrat avec la société Idemia pour une « solution d'empreintes digitales et de reconnaissance faciale en mode infonuagique privé [30].

En 2022, la SAAQ annonçait adopter elle aussi cette technologie, prétendument pour « faire le ménage » de sa banque de photos. Or, il s'avère difficile de connaître les détails de ce projet[31].

En novembre 2021, dans le cadre d'un avis sur le projet SAAQ, la CAI indiquait :

> « La Commission comprend aussi que la portée de ce projet dépasse la seule intégrité de la banque de photos liée à l'émission des permis de conduire. **Certaines affirmations de la SAAQ laissent entendre que cette banque pourrait être utilisée notamment dans le cadre du projet d'identité numérique du gouvernement du Québec ou pour offrir des services en ligne** ».

La CAI estime qu'un débat public est nécessaire : vu le caractère unique et permanent des données biométriques et des risques de discrimination et d'atteinte potentielle aux droits fondamentaux ; et du danger d'un détournement de finalité ou de piratage des données.

> « Pour ces raisons, la Commission est d'avis que ce projet devrait faire l'objet d'un débat public afin de permettre, en toute transparence, de présenter toutes les utilisations projetées de la reconnaissance faciale et de la banque de photos de la SAAQ, de mettre en lumière les enjeux liés à cette technologie ainsi que les avantages pour la SAAQ de l'utiliser.
>
> Le cas échéant, l'utilisation de la reconnaissance faciale par la SAAQ devrait être spécifiquement encadrée dans la loi de manière à baliser son utilisation et à protéger les droits des citoyens ».

Le 24 mars 2024, la CAI réitérait sa position[32]. Nous souscrivons entièrement à l'avis de la CAI.

Fonder un système d'identifiant gouvernemental sur l'utilisation de la biométrie mènerait à une banalisation insidieuse de cette technologie très invasive. Et ce, même si son usage demeurait facultatif.

L'encadrement législatif de cette technologie est insuffisant[33]. La reconnaissance faciale (RF) est probabiliste et peut conduire à des erreurs, particulièrement pour certains groupes (selon la couleur

---

biométrie dans les entreprises. Plus populaire, souvent illégal, La Presse, 14 octobre 2024. En ligne : https://www.lapresse.ca/actualites/usage-de-la-biometrie-dans-les-entreprises/plus-populaire-souvent-illegal/2024-10-14/une-banalisation-qui-suscite-l-inquietude.php

[30] Voir Sûreté du Québec, Réponse à une demande d'accès à l'information, 8 juin 2021. En ligne : https://www.sq.gouv.qc.ca/wp-content/uploads/2021/06/2021-06-08-contrat-societe-idemia.pdf

[31] Voir l'article de Nicolas Lachance, *Reconnaissance faciale à la SAAQ: Québec cache ses documents*, Journal de Québec, 3 septembre 2024. En ligne : https://www.journaldequebec.com/2024/09/03/reconnaissance-faciale-a-la-saaq--quebec-cache-ses-documents

[32] Commission d'accès à l'information, *SAAQ : projet d'acquisition d'une solution de reconnaissance faciale*, 26 mars 2024. En ligne : https://www.cai.gouv.qc.ca/actualites/saaq-projet-dacquisition-dune-solution-de-reconnaissance-faciale

[33] Voir Commission d'accès à l'information, *Projet de loi no 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Mémoire présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques, 29 septembre 2020. En ligne : https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PL-64.pdf

> « L'utilisation de plus en plus répandue de la biométrie soulève des enjeux importants pour la vie privée et la protection des renseignements personnels des individus. La législation actuelle ne permet pas d'encadrer adéquatement certaines utilisations de cette technologie. »

de la peau, l'âge, le sexe ou le handicap). Un incident de confidentialité impliquant de telles données pourrait entraîner des conséquences irréparables pour les individus concernés.

Par ailleurs, une fois la banque biométrique constituée, les autorités pourraient être tentées de l'utiliser à d'autres fins, comme le souligne la CAI dans son avis sur la SAAQ :

> « […] la constitution d'une banque de gabarits faciaux de plus de 5 millions de personnes qu'implique ce projet suscitera certainement la convoitise, tant de la part d'autres organismes publics, dont des autorités policières, que d'individus malveillants voulant tirer profit de la centralisation de ces renseignements particulièrement sensibles. Ces autres utilisations ou ces accès non autorisés risquent d'avoir des conséquences importantes pour les personnes concernées ».

Que l'utilisation de la biométrie demeure au choix des utilisateurs ne change pas notre position. Ce qui est volontaire un jour peut à terme devenir obligatoire. Et l'usage par l'État d'une technologie aussi intrusive ne relève pas seulement d'un choix personnel ; il met en cause un choix de société :

> « Ainsi, les limites de l'utilisation acceptable de la RF dépendent en partie des attentes que nous fixons aujourd'hui pour la protection de la vie privée dans le futur, dans un contexte où les capacités technologiques à transgresser les attentes raisonnables des Canadiens à l'égard de leur vie privée augmentent sans cesse[34] ».

D'ailleurs même le consentement de l'individu n'autorise pas un organisme à recourir à la biométrie si cela n'est pas nécessaire, comme le rappelle la CAI[35].

À tout le moins le sujet nécessite-t-il la tenue d'un débat public, franc et éclairé, où l'ensemble des projets seront mis sur la table et où citoyen-ne-s et experts pourront se faire entendre.

Il est inadmissible que le gouvernement puisse trancher la question par voie règlementaire, échappant ainsi à toute discussion.

4. Fracture numérique

Nous saluons le fait que l'enrôlement au système d'INN ne soit pas obligatoire pour l'accès aux prestations de services publics. L'article 10.3 du chapitre I.1 dispose en effet :

> 10.3. L'utilisation de l'identité numérique 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 façon dont l'État organise les services ne doit pas faire obstacle à l'exercice des droits des citoyen-ne-s. Selon une étude de l'Institut national de la recherche scientifique (INRS), un-e

---

[34] Commissariat à la protection de la vie privée du Canada, *Document d'orientation sur la protection de la vi privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, 2022. En ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/surveillance/police-et-securite-publique/gd_rf_202205/

[35] Commission d'accès à l'information, Biométrie, Consulté le 24 janvier 2025. En ligne : https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/biometrie

> « Même avec un consentement, le critère de nécessité doit impérativement être respecté pour commencer une collecte de renseignements biométriques. »

Québécois-e sur quatre (25 %) n'utilise pas les services gouvernementaux en ligne. L'INRS identifie sept principaux facteurs de vulnérabilité numérique : l'âge, la situation géographique, le revenu, les compétences numériques, le niveau d'éducation, le fait de vivre seul et le statut d'immigration[36].

Ce sont les groupes historiquement discriminés qui risquent de faire les frais de la transformation numérique gouvernementale, notamment les personnes âgées, en situation de handicap, à faible revenu, peu alphabétisées, autochtones ou immigrantes. Les femmes sont aussi moins portées à recourir aux services publics en ligne selon l'étude de l'INRS soit 69 % contre 80 % pour les hommes. Une étude de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) souligne :

> « La stratégie du *tout en ligne* risque d'exclure les personnes qui, pour diverses raisons, ne peuvent pas, voire ne veulent pas, être connectées et d'avoir de lourdes conséquences sur leur vie, surtout dans les domaines aussi sensibles que la justice[37] ».

En 2023, le Regroupement des groupes populaires en alphabétisation du Québec (RGPAQ) a déployé la campagne *Traversons l'écran. Pour un virage numérique humain*[38]. Cette campagne vise à alerter sur les conséquences de la transformation numérique des services publics sur les droits de la population. Elle insiste notamment sur la nécessité de maintenir des services en personne et des alternatives de qualité au tout numérique. Rappelons que 22 % des adultes âgés de 16 à 65 ans sont considérés peu alphabétisés au Québec[39] et que 16,4 % de la population est en situation de pauvreté[40].

Des solutions non numériques doivent exister pour les personnes n'ayant pas l'intérêt, les connaissances ou l'équipement nécessaires pour des services en ligne. Et l'alternative doit être réelle, sur le plan de la proximité et de la célérité des services. Des bureaux administratifs devraient être joignables partout au Québec.

Or, les cas de fermeture ou de réduction d'heures de bureau se multiplient, particulièrement à la SAAQ et la CNESST.[41] Nous craignons que le passage au gouvernement en ligne et la dématérialisation des services ne soit l'occasion de coupes importantes dans les services en

---

[36] Institut national de la recherche scientifique, *La fracture numérique : contexte québécois, pistes d'action et perspectives internationales*, Rapport final, mars 2024, p. 4. En ligne : https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/emploi-solidarite-sociale/publications-adm/rapport/RA_INRS_fracture_num.pdf

[37] Alexis, A., Bahary-Dionne, A. (2022). Réduire les impacts de la fracture numérique sur les populations marginalisées : leçons apprises de la littérature à la portée des organismes communautaires, Observatoire international sur les impacts sociétaux de l'IA et du numérique, Québec, 73p. à la p.36. En ligne https://www.obvia.ca/sites/obvia.ca/files/ressources/202209-OBV-Pub-ImpactsFractureNumerique.pdf

[38] Regroupement des groupes populaires en alphabétisation du Québec, *Traversons l'écran – Pour un virage numérique humain*, Campagne. En ligne : https://rgpaq.qc.ca/traversons

[39] *Programme pour l'évaluation internationale des compétences des adultes (PEICA), 2022.*

[40] Lena A. Hübner, Martin Bonnard et Normand Landry, *La pauvreté au Québec : portrait, bilan et perspectives*, Manuscrit non publié, Université TÉLUQ, 2020, page 8. URL : https://r-libre.teluq.ca/2158

[41] Radio-Canada, Un syndicat dénonce la fermeture de bureaux de la CNESST dans l'Est-du-Québec, Radio-Canada, 27 septembre 2022. En ligne : https://ici.radio-canada.ca/nouvelle/1919674/fermeture-bureau-service-fonction-publique ; Voir aussi François Morin, *Fermeture partielle du bureau de Services Québec à Saint-Jean-de-Matha*, CFNJ 99,1 FM, 9 octobre 2024. En ligne : https://cfnj.net/fermeture-partielle-du-bureau-de-services-quebec-a-saint-jean-de-matha ; Charles Ferron, *Fermeture des bureaux de la SAAQ: surprise et déception à Magog*, La Tribune, 17 décembre 2024. En ligne : https://www.latribune.ca/actualites/actualites-locales/estrie-et-regions/2024/12/17/fermeture-des-bureaux-de-la-saaq-surprise-et-deception-a-magog-JB6RY3WFLZBCLCG5MY46EX3OIE ; Carl Sincennes, *Fermeture du bureau de la SAAQ à LaSalle*, Nouvelles d'Ici, 9 décembre 2024. En ligne : https://nouvellesdici.com/actu/fermeture-bureau-saaq-lasalle

personne ou par téléphone, menant à une accentuation inacceptable de la discrimination technologique et de l'exclusion sociale qu'ils entrainent déjà.

Par ailleurs, si les organismes publics ne peuvent exiger l'INN, qu'en sera-t-il du secteur privé ? On sait qu'un portefeuille numérique permettant « de réaliser des interactions dans la collectivité, notamment à l'aide d'attestations numériques gouvernementales [42]» sera disponible pour des transactions avec des entreprises privées. Il importe que l'INN ne soit pas exigible non plus dans le secteur privé. Comme le stipule le Règlement européen sur l'identité numérique :

> « Les utilisateurs ne devraient pas être tenus d'utiliser un portefeuille européen d'identité numérique pour accéder à des services privés et ne devraient pas être limités ou entravés dans leur accès aux services au motif qu'ils n'utilisent pas de portefeuille européen d'identité numérique[43] ».

L'anonymat doit en outre pouvoir être sauvegardé lorsque l'identité réelle ou juridique n'est pas nécessaire :

> « Le recours à l'identité juridique ne devrait pas empêcher les utilisateurs de portefeuilles européens d'identité numérique d'accéder aux services sous un pseudonyme, dès lors que l'identité juridique n'est pas requise pour l'authentification[44] ».

Le PL 82 devrait prévoir des dispositions en ce sens.

5. Pouvoirs règlementaires

Le PL 82 accorde au gouvernement ou au ministre de larges pouvoirs règlementaires ou normatifs.

Ainsi, aux quelques données numériques gouvernementales (DNG) définies à l'article 10.6 (nom, date de naissance, nom des parents), le gouvernement pourrait ajouter « tout autre renseignement » qu'il détermine. Aussi bien dire que les DNG, un élément pourtant essentiel aux fins de l'INN, ne sont pas déterminées dans la loi. Qui plus est, l'ajout pourrait se faire apparemment par simple décret.

Le PL 82 précise à l'article 10.7 les fonctions du RINN (conservation, communication, accès et traçabilité d'accès aux DNG). Le ministre pourrait attribuer à ce registre « toute autre fonctionnalité déterminée par règlement ». Il s'agit là encore d'une carte blanche sur un élément fondamental du système.

Le gouvernement se voit aussi autorisé, par l'article 10.9, à fixer par règlement : les modalités de tenue du registre ; les normes de qualité et de protection des DNG ; les DNG ayant des caractéristiques biométriques pouvant être utilisées (pouvoir critiqué précédemment) ; **et toute autre mesure nécessaire à l'application du chapitre I.1.**

L'ensemble de ces dispositions confère une discrétion démesurée au pouvoir exécutif sur des items primordiaux. Nous estimons que tant les DNG que les fonctionnalités du registre doivent être

[42] Article 10.2 (al.2) du chapitre I.1 (article 6 du PL 82).

[43] Règlement (UE) 2024/1183 du Parlement européen et du Conseil modifiant le règlement (UE) no 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique, 11 avril 2024, par. 57. En ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401183

[44] Idem, par. 19.

inscrites à la loi. Quant au pouvoir d'adopter toute autre mesure pour l'application du chapitre sur l'INN, il apparaît exorbitant.

6. Interopérabilité

Notons enfin le pouvoir du gouvernement de déterminer les conditions d'une entente pour rendre l'INN interopérable avec les systèmes de toute autre personne ou entité sur le plan local, régional, national ou international.

Puisque l'interopérabilité comporte des risques pour la vie privée et la sécurité des données, et encore davantage si l'INN devait comporter des données biométriques, il nous paraît essentiel que celle-ci soit limitée au minimum, sa nécessité justifiée et strictement démontrée, et qu'elle soit encadrée juridiquement. De plus, elle doit nécessiter le consentement de la personne, afin de ne pas porter atteinte aux droits humains en matière de confidentialité et de ne pas exposer les données personnelles aux risques de vol et d'utilisation abusive.

Une interopérabilité avec toute personne ou entité tant locale qu'internationale, sans critères ni restrictions prédéfinies, paraît excessivement large et hasardeuse. Au minimum, l'interopérabilité doit préalablement et obligatoirement exclure toute personne ou entité, étatique ou privée, qui ne respecte pas les droits humains et les droits à la vie privée, ou qui aurait commis ou facilité de graves violations à cet égard.

Cette notion d'interopérabilité devrait être précisée et développée dans la loi et ne pas être laissée à la seule appréciation du gouvernement.

7. Portefeuille numérique

L'INN doit permettre l'accès sécurisé aux prestations électroniques de services gouvernementales. Elle compte aussi un volet permettant « de réaliser des interactions dans la collectivité, notamment à l'aide d'attestations numériques gouvernementales [...] à partir d'une application[45] ». C'est le fameux portefeuille numérique sur lequel le PL 82 est pratiquement muet.

Le mémoire au Conseil des ministres sur le programme SQIN (décembre 2021) évoque le « triangle de confiance » que forment « l'émetteur d'un document, le détenteur de celui-ci et celui qui le consomme »[46]. Autrement dit le gouvernement (émetteur), le ou la citoyen-ne (détenteur) et l'organisme public ou l'entreprise privée (consommateur).

Le mémoire détaille ensuite les avantages de cet écosystème (public et privé) pour le consommateur de l'INN, à savoir les organismes publics et les entreprises privées : moyen fiable et légalement reconnu de valider l'identité d'un-e résident-e du Québec avec lequel ils souhaitent faire affaire ; les consommateurs de l'INN pourront bénéficier d'une gouvernance dans laquelle ils trouveront le niveau de confiance recherché en plus d'être soutenus et accompagnés. Le document indique encore que les entreprises ont été consultées :

[45] Article 10.2 (al.2) du chapitre I.1 (article 6 du PL 82).

[46] Gouvernement du Québec, *op. cit.*, note 1, p. 4.

> « De plus, des entreprises couvrant plusieurs domaines d'affaires (finances, télécommunications, assurances) ont été consultées étant donné la couverture du projet (écosystème public et privé). L'objectif de ces consultations était de recueillir ou de valider les besoins qui font partie intégrante de la solution proposée.[47] »

Le portefeuille numérique parait donc répondre d'abord aux besoins de l'entreprise privée. Est-ce bien là une mission de l'État ? Le secteur privé contribuera-t-il financièrement à ce réseau de confiance ? Quelle gouvernance prévoit-on ? Les entreprises devront-elles signer un contrat pour l'utilisation du portefeuille ?

Du côté du citoyen, qu'en sera-t-il du traçage de ses transactions ? De la durée de conservation de celles-ci ? De l'accès aux données et du droit de retrait du service ? Des responsabilités en cas d'usurpation d'identité ou autre fraude ? Du droit ou non des entreprises d'exiger l'utilisation du portefeuille ? Autant de questions sans réponses.

Conclusion

L'INN devrait être conçue de manière à garantir la protection des renseignements personnels. Elle doit servir au renforcement des droits humains, et non permettre la surveillance (étatique ou privée) ou conduire à la discrimination ou à l'exclusion. Elle doit augmenter la sécurité des échanges en ligne et non fragiliser la protection d'informations personnelles névralgiques. Pour la LDL, plusieurs éléments du PL 82 n'atteignent pas ces objectifs, en plus d'accorder au ministre de larges pouvoirs règlementaires ou normatifs de déterminer certaines modalités pourtant très importantes, échappant ainsi à tout débat public.

La banque centralisée de renseignements personnels aux fins de l'INN ; le recours éventuel à la biométrie ; le manque d'encadrement sur le plan de l'interopérabilité avec d'autres systèmes : autant d'éléments qui, selon nous, mettent à risque des données personnelles sensibles et peuvent conduire à des dérives.

Par ailleurs, le gouvernement poursuit sa transformation numérique à marche forcée. Tout cela n'augure rien de bon pour les groupes historiquement discriminés qui sont confrontés à des formes d'exclusion numérique, aussi appelées fractures numériques. Si l'INN demeure optionnelle, rien d'autre au PL 82 ne garantit que des services traditionnels seront disponibles au choix des individus et dans des conditions de concurrence équitables avec les services en ligne. Le passage au numérique risque de compliquer, voire de compromettre l'exercice de nombreux droits économiques et sociaux et l'accès à des prestations ; entraînant par là une forme d'exclusion numérique et le creusement d'inégalités.

Il reste encore beaucoup trop d'inconnu dans le projet d'identité numérique gouvernementale, notamment en ce qui concerne le portefeuille numérique. Nous réclamons un véritable débat sur l'architecture de cet outil, son mode de fonctionnement et de gouvernance, son utilité et son financement.

[47] Gouvernement du Québec, *op. cit.*, note 1, p. 8.

Résumé de nos demandes

1. La LDL demande la tenue d'un débat public informé, éclairé et transparent sur l'ensemble du projet gouvernemental d'identité numérique incluant le portefeuille numérique (architecture de cet outil, mode de fonctionnement et de gouvernance, utilité, financement, interopérabilité, effets sociaux et sur les droits humains, etc.) Un tel débat public doit permettre aux citoyen-nes et aux expert-es de se faire entendre et de discuter des choix faits par le gouvernement (une consultation en ligne ne répond pas à cette exigence) ;
2. La LDL s'inquiète de la création d'un registre centralisé de renseignements personnels aux fins de l'Identité numérique nationale (INN) ;
3. La LDL demande que le système d'INN soit dédié exclusivement à l'identification et l'authentification des personnes. La loi devrait interdire toute autre utilisation, par quiconque ;
4. La LDL s'oppose à l'utilisation de la biométrie aux fins de l'INN et demande le retrait en conséquence des pouvoirs règlementaires prévus au paragraphe 3 de l'article 10.9 du chapitre I.1 ;
5. La LDL demande la tenue d'un débat public sur l'ensemble des projets gouvernementaux en cours relativement à l'utilisation de la biométrie (notamment Sûreté du Québec, Société de l'assurance automobile du Québec, ministère de la Cybersécurité et du Numérique) ;
6. La LDL demande que les services gouvernementaux restent accessibles en mode traditionnel, et ce, dans des conditions de concurrence équitables avec les services en ligne ;
7. La LDL demande que l'usage de l'INN ne puisse être imposé dans le cadre de transactions dans la collectivité ;
8. La LDL demande le retrait des pouvoirs règlementaires ou normatifs prévus aux articles suivants du chapitre I.1 de la *Loi sur le ministère de la Cybersécurité et du Numérique* (article 6 du PL 82) :
    - 10.6, al.4, par.3 ;
    - 10.7 al. 2, par.5 ;
    - 10.9 par.4 ;
9. La LDL demande l'encadrement dans la loi des conditions et modalités permettant de rendre l'INN interopérable avec d'autres systèmes ; et exclure toute personne ou entité, étatique ou privée, qui ne respecte pas les droits humains et les droits à la vie privée.