

**MÉMOIRE DE LA COMMISSION DE L'ÉTHIQUE
EN SCIENCE ET EN TECHNOLOGIE**

**Consultations particulières et auditions publiques sur le projet de loi n° 82, *Loi
concernant l'identité numérique nationale et modifiant d'autres dispositions***

Présenté à la Commission des finances publiques
Assemblée nationale du Québec

Janvier 2025

Document préparé par

Kathia Légaré, conseillère en éthique

Guillaume Pelletier, conseiller en éthique

Coordination

Nicolas Bernier, Secrétaire général par intérim

Direction

Luc Bégin, président de la CEST

Commission de l'éthique en science et en technologie

888, rue Saint-Jean, bureau 555

Québec, QC

G1R 5H6

www.ethique.gouv.qc.ca

Table des matières

Présentation de la Commission de l'éthique en science et en technologie	1
Remarques générales	2
Commentaires spécifiques au projet de loi	2
Transparence et enjeux démocratiques	2
Interdiction du profilage	4
Service d'authentification et traçabilité des transactions.....	4
Enjeux éthiques relatifs à la mise en œuvre du projet de loi	5
Autonomie et souveraineté numérique	5
Littératie numérique et accès aux services gouvernementaux	6

Présentation de la Commission de l'éthique en science et en technologie

La Commission de l'éthique en science et en technologie (CEST) est un organisme du gouvernement du Québec placé sous la responsabilité du ministre de l'Économie, de l'Innovation et de l'Énergie. Elle est composée de 13 membres, dont un président, nommés par le gouvernement.

Sa mission est de conseiller la ministre et le gouvernement sur toute question relative aux enjeux éthiques liés à la science et à la technologie, ainsi que de susciter la réflexion sur ces enjeux éthiques. De façon générale, ses activités visent à informer, à sensibiliser et à émettre des recommandations autour des enjeux éthiques en science et en technologie. La CEST propose également des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.

Les analyses qui suivent s'inscrivent dans un ensemble plus large de travaux menés par la CEST dans le contexte des changements législatifs en cours dans le domaine du numérique. En particulier, la CEST a publié en octobre 2022 un avis portant sur les enjeux éthiques liés à la gestion et à la valorisation des données de santé¹, et en août 2023 un avis portant sur la transformation numérique du réseau de la santé et des services sociaux en vue d'intégrer l'intelligence artificielle². Les commentaires et propositions de modifications au projet de loi n° 82 proposés dans le présent mémoire reprennent en partie les orientations et recommandations de ces avis.

Ces commentaires ont été préparés par le secrétariat de la CEST et par son président. N'ayant pas fait l'objet d'une résolution lors d'une réunion officielle des membres, ces commentaires ne sont pas une publication officielle de la CEST.

¹ CEST (2022). *Mériter et renforcer la confiance des citoyens dans la gestion et la valorisation des données de santé*, Gouvernement du Québec.

<https://www.ethique.gouv.qc.ca/fr/publications/meriter-et-renforcer-la-confiance-des-citoyens-dans-la-gestion-et-la-valorisation-des-donnees-de-sante/>

² CEST (2023). *La transformation numérique du réseau de la santé et des services sociaux en vue d'intégrer l'intelligence artificielle : un regard éthique*, Gouvernement du Québec.

<https://ethique.gouv.qc.ca/fr/publications/la-transformation-numerique-du-reseau-de-la-sante-et-des-services-sociaux-en-vue-d-integrer-l-intelligence-artificielle-un-regard-ethique/>

Remarques générales

La CEST accueille favorablement la volonté d'assurer la sécurité des renseignements personnels détenus par le gouvernement, de simplifier les démarches d'authentification pour les citoyennes et citoyens et de favoriser l'efficacité et l'efficacités des services gouvernementaux. Elle souligne toutefois certains risques liés à la forme actuelle du projet de loi et à sa mise en œuvre qui pourraient avoir un impact négatif sur la relation de confiance entre les citoyennes et citoyens et les instances gouvernementales.

Dans son avis sur les données de santé (2022), la CEST plaçait la **confiance** au centre de son analyse éthique, en soulignant son caractère primordial dans la gestion des données des citoyennes et des citoyens. Or, le contexte actuel est marqué par une certaine crise de confiance envers les institutions, particulièrement en ce qui concerne la gestion des renseignements personnels. Diverses raisons peuvent expliquer cette crise de confiance, notamment des incidents liés à la mise en œuvre de projets numériques ou à la cybersécurité lors des dernières années, tant du côté d'organisations publiques que privées.

Dans le même avis, la CEST soutenait que « **la confiance ne peut pas être tenue pour acquise, mais doit plutôt être activement gagnée, méritée, favorisée et maintenue par les institutions fiduciaires des données des citoyens** » (CEST, 2022, p. 24). Pour mériter cette confiance, diverses actions et divers mécanismes assurant la transparence et l'imputabilité des parties prenantes doivent être mis en place (ex. : mesures de traçabilité, registres d'utilisation des données, mesures de surveillance). À ce titre, la CEST identifie dans le projet de loi certains aspects qui posent des problèmes ou qui pourraient être améliorés au regard de ces principes.

Commentaires spécifiques au projet de loi

Transparence et enjeux démocratiques

De manière générale, on observe qu'un nombre important de précisions concernant notamment **la mise en œuvre du registre de l'identité numérique nationale** seront à définir par voie de règlement. Cette procédure assure une certaine flexibilité au projet de loi, mais laisse toutefois une discrétion importante au ministre, en plus de rendre difficile l'examen démocratique de certains aspects essentiels à la mise en place du registre.

À ce titre, le projet de loi laisse en suspens plusieurs précisions importantes, notamment au regard :

- *Des renseignements concernés par le registre* : Le projet de loi prévoit que les données numériques gouvernementales peuvent inclure « tout autre renseignement que détermine le gouvernement » (**Article 6, « 10.6, 3e alinéa »**)
- *Des finalités du registre* : Le projet de loi prévoit que le registre doit permettre « toute autre fonctionnalité déterminée par règlement du ministre ». (**Article 6, « 10.7, 5e alinéa »**)

- *De la mise en œuvre du registre* : Le projet de loi prévoit que le gouvernement pourra déterminer par règlement les modalités de tenue du registre, les normes de qualité et de protection des données, les caractéristiques biométriques utilisables pour le registre ; ainsi que la prescription de « toute autre mesure nécessaire à l'application du présent chapitre ». (**Article 6, « 10.9, 4^e alinéa »**)
- *Des règles relatives à l'identification et à l'authentification des personnes* : Le projet de loi prévoit que le ministre pourra prévoir ces règles par règlement. (**article 6, « 10.10 »**)

Or, ces différents aspects à déterminer par règlement sont essentiels et **mériteraient un examen démocratique transparent et élargi**. La formulation actuelle et la place accordée aux règlements laissent de trop grandes imprécisions quant aux finalités du registre qui sera mis en place, et risquent par le fait même d'alimenter, au sein de la population, la spéculation ou même la désinformation sur les usages du registre. À l'inverse, apporter davantage de précisions en amont participerait au maintien d'un climat de confiance dans la gestion des données des citoyennes et des citoyens.

Par ailleurs, selon le tableau de bord des projets en ressources informationnelles³, le niveau d'avancement du SQIN est évalué à 50 %. Toutefois, il faut constater qu'il est encore difficile de trouver des informations précises sur le programme et sur son orientation globale. Par exemple, on retrouve peu d'explications et de justifications quant aux modèles de gestion des données qui ont été priorisés. En effet, le SQIN vise à donner aux citoyens et aux citoyennes le contrôle de leurs données, notamment en leur permettant de conserver eux-mêmes leurs attestations numériques. Toutefois, le projet de loi actuel formalise la création d'un registre constitué de données des citoyens et des citoyennes détenues par la RAMQ qui, selon notre compréhension du projet, correspond à un modèle centralisé. Étant donné les différents modèles existants⁴ et les risques qui leur sont associés⁵, **il serait souhaitable de présenter et d'expliquer plus clairement les choix qui ont été faits en matière d'architecture**.

Notons enfin que les enjeux de transparence mentionnés ci-haut sont accentués par le fait que, depuis les modifications apportées à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* en 2023, il n'existe plus d'exigence d'approbation des règles de gouvernance des renseignements personnels du MCN par la Commission d'accès à l'information (CAI)⁶.

³ [Projets- Tableau de bord des projets de l'administration publique](#)

⁴ « Les solutions d'identification et d'authentification se présentent sous une variété de formes allant de la centralisation totale, où un serveur central (par exemple : en utilisant un compte en ligne) est non seulement la référence, mais aussi nécessaire à toute identification ou authentification, à des solutions plus décentralisées pour lesquelles l'identification peut se faire indépendamment d'une base centrale (par exemple lorsqu'on prouve son identité en magasin avec une pièce d'identité). » Commission nationale de l'informatique et des libertés (CNIL- France), *L'identité numérique*, Dossier thématique, 2023, p. 13

⁵ Par exemple, les organismes de surveillance du Canada se prononçaient en 2022 contre la mise en place d'une base de données centralisée dans le contexte de l'identité numérique : [Identité numérique au... | Commission d'accès à l'information du Québec](#)

⁶ En effet, le PL38, sanctionné en décembre 2023, autorise « le retrait de l'obligation, pour un organisme public désigné comme source officielle de données numériques gouvernementales [le

Interdiction du profilage

La CEST accueille favorablement l'inclusion dans le projet de loi d'une interdiction claire du profilage des personnes (**article 6, « 10.7 »**). Toutefois il serait souhaitable d'élargir la définition proposée afin qu'elle ne se limite pas à sa dimension individuelle. En effet, comme le soulignait la CEST dans son mémoire sur le projet de loi n° 64, il est tout à fait possible d'effectuer du profilage qui n'identifie à aucun moment une personne physique, mais qui aura des incidences sur des catégories de personnes dont les intérêts et les droits devraient néanmoins être protégés (**profilage social**)⁷. Par exemple, on pourrait imaginer le recours à des ensembles de données anonymisées, tirées du registre, pour établir un profil par quartier de manière à « optimiser » ou « préciser » des politiques de sécurité publique. Même si aucune personne physique n'est directement identifiée, ce type de profilage pourrait entraîner des répercussions importantes pour les groupes auxquels ces personnes appartiennent, telles que des risques de stigmatisation.

Il pourrait par ailleurs être opportun de ne pas limiter cette interdiction au ministre, par exemple en remplaçant « le ministre » par « le gouvernement ».

Service d'authentification et traçabilité des transactions

Le projet de loi prévoit que l'identité numérique permettra « des interactions dans la collectivité, notamment à l'aide d'attestations numériques gouvernementales dont elle détient le contrôle à partir d'une application où ces attestations sont déposées de façon sécurisée » (**article 6, « 10.2 »**), et donc que les attestations concernées pourraient être mobilisées non seulement dans le cadre de services publics, mais lors de transactions privées.

Cet aspect du projet de loi soulève des enjeux éthiques importants et mériterait davantage de balises et de précisions. Par exemple, quels types d'utilisation sont envisagés par ces « interactions dans la collectivité » ? Le projet de loi prévoit qu'un organisme public ne pourra pas exiger le recours à l'identité numérique pour offrir des services à la population (**article 6, « 10.3 »**), mais il ne semble pas en être de même pour le privé. Or, l'obligation de s'identifier par le biais de l'identité numérique pour avoir accès à certains services privés pourrait exercer une pression indue sur les usagers et les usagères et mener, dans un contexte de fracture numérique, à certaines iniquités.

MCN], de faire approuver par la Commission [la CAI] les règles qu'il doit établir concernant sa gouvernance des renseignements personnels visés, préalablement à toute collecte, utilisation ou communication de celles-ci. Cette obligation est remplacée par l'obligation de les transmettre à la Commission uniquement. » La CEST avait soulevé des inquiétudes à cet égard dans un commentaire envoyé sur le projet de loi en question. La CAI avait quant à elle recommandé le maintien de cette obligation : https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ME_PL-38.pdf

⁷ Mémoire de la CEST sur le projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (2022).

De plus, le Service d'authentification en cours de déploiement conserve et utilise divers renseignements à des fins techniques et statistiques, en particulier l'adresse IP pour géolocaliser l'appareil utilisé (ville et pays). Le consentement de l'utilisateur ou de l'utilisatrice à la collecte de ces renseignements est une condition obligatoire pour avoir accès au service⁸. En théorie, le SQIN est soumis aux règles de renseignements personnels, et la conservation est donc limitée. Toutefois, le projet de loi ne précise pas si les différentes transactions effectuées à l'aide d'une attestation numérique seraient traçables ou si elles seraient détruites. Or, cet aspect pose d'importants enjeux **de protection de la vie privée** : pensons par exemple aux transactions qui pourraient être effectuées lors de recours aux attestations numériques auprès de banques ou encore dans le cadre d'arrestations policières.

Ces nombreux questionnements concernant l'usage d'attestations numériques mériteraient d'être précisés et soumis au débat public. Étant donné la sensibilité de telles données, et afin de préserver la confiance du public, **ne devrait-il pas y avoir un engagement à ce que le système québécois d'identité numérique ne permette pas de faire le suivi des activités des personnes à travers l'archivage de leurs transactions ?**

Enjeux éthiques relatifs à la mise en œuvre du projet de loi

Autonomie et souveraineté numérique

Dans son avis sur la transformation numérique du réseau de la santé et des services sociaux en vue d'intégrer l'intelligence artificielle (2023), la CEST soulignait l'importance d'assurer **l'autonomie des organismes publics** par rapport au secteur privé dans le domaine des TI. À cet égard, le projet d'identité numérique pourrait soulever les inquiétudes suivantes :

Expertise interne : Nous sommes actuellement dans un contexte où le gouvernement éprouve des difficultés à recruter une expertise interne hautement qualifiée en TI. Or, l'importance de cette expertise dans le contexte de la gestion d'une identité numérique nationale est non seulement une question d'efficacité et de qualité des services publics, mais aussi une question **d'imputabilité** et **d'autodétermination** des organismes publics par rapport aux fournisseurs et aux consultants externes.

Souveraineté des données : La question de savoir où seront hébergées les données de l'identité nationale est aussi cruciale. La dépendance à des géants américains comme Microsoft ou Amazon (AWS) pourrait exacerber les inquiétudes de la population liées aux fuites de données sensibles⁹, en plus de soulever des enjeux de cybersécurité à l'échelle collective advenant un accroissement des tensions politiques entre les deux États.

⁸ <https://contenu.authentification.quebec.ca/politique-confidentialite/politique-confidentialite.html>

⁹ À l'heure actuelle, selon la politique de confidentialité du service d'authentification gouvernementale : « Dans certains cas, les infrastructures de ces tiers sont situées à l'extérieur du

Littératie numérique et accès aux services gouvernementaux

Certains facteurs, comme la fracture numérique ou une faible connaissance des enjeux liés aux données, font qu'il est actuellement difficile d'attendre de chaque personne qu'elle soit en mesure d'avoir recours par elle-même aux attestations numériques gouvernementales. Ainsi, la mise en place de ces attestations **ne doit pas faire en sorte de limiter l'accès aux personnes concernées par cette fracture numérique aux services publics**. Il est vrai que le projet de loi prévoit que le recours à ces attestations demeurera optionnel dans le secteur public (**article 6, « 10.3 »**), mais le gouvernement devra s'assurer que ce principe soit bel et bien respecté et que la disponibilité d'attestations numériques ne conduise pas certains ministères ou organismes à diminuer ou délaisser les solutions alternatives.

Le succès de cette mesure sera par ailleurs tributaire des efforts en matière d'accessibilité, de sensibilisation, et d'information qui concerneront les modalités de déploiement de ces attestations numériques. À l'heure actuelle, le pourcentage de citoyennes et de citoyens qui utilisent le service d'authentification numérique est en deçà de l'objectif fixé par le gouvernement¹⁰.

Québec. Le cas échéant, avant de transmettre vos renseignements personnels à ces tiers, nous prenons des mesures de protection. Nous réalisons une évaluation des facteurs relatifs à la vie privée, une démarche où nous considérons tous les facteurs qui peuvent avoir un impact sur votre vie privée et évaluons si vos renseignements personnels seront adéquatement protégés. Lorsque nous concluons des contrats ou des ententes avec ces tiers, nous nous assurons que vos renseignements personnels soient protégés, en incluant notamment des mesures de sécurité adéquates. » [Politique de confidentialité | Service d'authentification gouvernementale](#)

¹⁰ MCN, Rapport annuel de gestion 2023-2024, 2024, p. 9.