Encadrer l'usage de l'IA dans les services publics : enjeux et recommandations

Mémoire de l'Obvia déposé au Protecteur du citoyen

Direction Collaboration avec la société civile
Direction Collaboration avec les acteurs publics

obvia

Juillet 2026

Rédaction

Lyne Nantel
Conseillère en engagement citoyen et collaboration avec la société civile, Obvia

Esther Poisson
Conseillère en affaires gouvernementales et relations avec les acteurs publics, Obvia

Révision scientifique

Karine Gentelet
Professeure agrégée, Département des sciences sociales, Université du Québec en Outaouais (UQO)
Directrice scientifique, Collaboration avec la société civile, Obvia

Hugo Loiseau
Professeur titulaire, École de politique appliquée, Membre du Pôle d'expertises en cybersécurité, Université de Sherbrooke
Directeur scientifique, Collaboration avec les acteurs publics, Obvia

L'Obvia est un réseau de recherche financé par le Fonds de Recherche du Québec qui mène des recherches indépendantes et interdisciplinaires en plaçant l'humain au cœur du développement technologique. Sa communauté regroupe plus de 300 chercheurs provenant des domaines des sciences humaines et sociales, des sciences et de l'ingénierie, ainsi que de la santé. À travers une approche intersectorielle, l'Obvia offre un espace ouvert pour la réflexion critique et la délibération démocratique. En collaboration avec la société civile, les institutions publiques, l'industrie et les développeurs, notre communauté produit des connaissances ouvertes qui renforcent les capacités individuelles et collectives.

obvia.ca

Les activités et travaux de recherche de l'Obvia – Observatoire international sur les impacts sociétaux de l'IA et du numérique sont rendus possibles grâce à une subvention du Fonds de recherche du Québec.

Pour citer ce document : Nantel, L., Poisson, E., Gentelet, K. et Loiseau, H. (2026). *Encadrer l'usage de l'IA dans les services publics : enjeux et recommandations – Mémoire de l'Obvia déposé au Protecteur du citoyen.* Obvia. https://doi.org/10.61737/AQDK8802

ISBN : 978-2-925581-46-8
DOI : 10.61737/AQDK8802

Table des matières

Sommaire 4

Mise en contexte 5

Section 1 - Fractures numériques : inégalités et exclusions face à la numérisation des services publics 7

Section 2 - Protection des renseignements personnels, droit à la vie privée et acceptabilité sociale 9

Section 3 - L'automatisation des services avec l'IA : équité, biais et contrôle humain 13

Conclusion 15

Sommaire

Principaux enjeux et risques identifiés

Fracture numérique et exclusion des populations vulnérables

L'IA et la numérisation des services publics risquent d'accentuer les inégalités sociétales déjà existantes. Les personnes ayant un accès limité aux technologies, un manque de littératie numérique ou étant en situation de vulnérabilité socioéconomique peuvent éprouver davantage de difficulté à accéder aux services, à comprendre les décisions automatisées ou à faire valoir leurs droits.

Risques pour la vie privée et la protection des renseignements personnels

L'utilisation accrue de systèmes numériques et d'IA entraîne des risques liés à la collecte, à la centralisation, au partage et à l'hébergement des données personnelles. Le recours à des fournisseurs externes et la possibilité de croisement automatisé des données soulèvent des préoccupations en matière de confidentialité, de profilage et de surveillance.

Déficit de confiance et d'acceptabilité sociale

Une partie importante de la population demeure méfiante envers l'utilisation de l'IA par le gouvernement. L'opacité, la compréhension limitée du fonctionnement des systèmes, le manque de consultation des personnes citoyennes et les doutes quant à la capacité du gouvernement à protéger les données et à gérer adéquatement les systèmes fragilisent la confiance citoyenne.

Déshumanisation des services, biais algorithmiques et perte de contrôle humain

L'automatisation croissante des décisions administratives peut réduire la qualité des services dans les situations complexes, faire disparaître l'accompagnement personnalisé et amplifier les conséquences d'erreurs administratives, notamment en raison des différents biais algorithmiques.

Recommandations

1 Favoriser une approche inclusive de la transformation numérique

- Penser l'adoption en fonction des besoins exprimés sur le terrain et des bénéfices pour les prestataires de services
- S'assurer de rejoindre des publics variés et pouvant être plus éloignés du numérique dans les services numériques intégrant l'IA
- Intégrer des pratiques de conception inclusive, comme des alternatives hors ligne réellement équivalentes aux services numériques en matière d'accessibilité, de délais et de qualité

2 Renforcer la transparence et la protection des données

- Baliser clairement le recours à la sous-traitance et aux partenariats publics-privés et permettre des audits indépendants en matière de sécurité et de protection des renseignements personnels
- Réaliser systématiquement des évaluations des facteurs relatifs à la vie privée dès la conception des projets et faire preuve d'une grande prudence dans l'octroi de contrats à des fournisseurs étrangers
- Adapter les pratiques de gestion des données pour des groupes tels que les Premiers Peuples afin de refléter leurs droits à l'autodétermination et les principes qu'ils ont développé concernant leurs données

3 Miser sur la confiance et la participation citoyenne

- Mieux informer les personnes citoyennes sur le fonctionnement, les avantages et les limites des systèmes d'IA
- Créer des espaces permanents et formels de dialogue citoyen sur le déploiement de l'IA dans les services publics
- Reconnaître et intégrer les expertises citoyennes et de terrain dans l'évaluation des besoins et des projets

4 Préserver l'équité et le contrôle humain

- Développer la littératie de l'IA et du numérique au sein de la fonction publique pour favoriser un jugement critique éclairé dans les décisions assistées par l'IA
- Prévoir des mécanismes clairs et accessibles pour identifier, contester et corriger les erreurs algorithmiques
- Assurer que les systèmes d'IA demeurent encadrés par des principes de transparence, de contrôle, d'imputabilité et de reddition de comptes tout au long de leur cycle de vie

Mise en contexte

L'optimisation et le renouvellement des services publics par l'intelligence artificielle sont au cœur de la *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021-2026*[1] du gouvernement du Québec. Le recours à l'intelligence artificielle (IA) dans les services publics, qui s'inscrit en continuité de la numérisation de ces services, est motivé notamment par l'objectif d'améliorer leur efficacité et la qualité du service. L'IA est destinée à plusieurs fins, par exemple pour fluidifier le contact avec les citoyens et les citoyennes via notamment des agents conversationnels, pour faciliter l'analyse de demandes et de dossiers, pour soutenir la prise de décision ou encore pour établir des tendances et faire des prédictions[2].

Nous n'en sommes qu'aux débuts de l'IA dans les services publics. À ce jour, le *Portrait public de l'utilisation des systèmes d'intelligence artificielle au Québec* répertorie deux cent cinquante-huit (258) algorithmes dans l'administration publique, tous ministères confondus[3]. On peut y retrouver une variété d'applications, comme des algorithmes utilisés pour « soutenir la prévention du décrochage scolaire » dans le domaine de l'éducation, des outils d'« aide à la sélection des dossiers à examiner » au Curateur public du Québec et un dispositif pour « l'évaluation, la détection et la priorisation des dossiers à risques de non-conformité fiscale » au sein de Revenu Québec[4].

Selon le gouvernement du Québec, les outils d'IA ont le potentiel de générer de l'efficience et de la cohérence dans les décisions; cependant, au vu des travaux menés par la communauté des chercheuses et des chercheurs de l'Obvia, les risques sont bien réels. À cet égard, l'Obvia s'appuie notamment sur les principes portés par la Déclaration de Montréal[5] pour un développement responsable de l'IA, dont ceux relatifs à l'équité, à la protection de la vie privée, à la participation démocratique, à la responsabilité et à la prudence[6].

Parmi la liste des enjeux et des risques les plus importants associés à l'usage de l'IA dans les services publics, nous souhaitons mettre en lumière les suivants:

- L'accélération de la fracture numérique et le droit d'accès aux services publics;
- Le déficit d'accès et l'exclusion de groupes ou d'individus en situation de vulnérabilité;
- Le droit à la vie privée et la protection des renseignements personnels;
- Le manque de transparence et l'impact sur le droit à l'information, à l'explication et à la reddition de comptes;
- L'automatisation excessive et la déshumanisation des décisions, limitant la capacité à traiter des dossiers complexes;
- Les biais, les discriminations algorithmiques et le risque pour le droit à l'égalité.

Pour consulter des ressources qui traitent en profondeur des différents enjeux de l'IA dans les services publics, nous vous invitons à visiter le répertoire des ressources de l'Obvia.

1 Gouvernement du Québec (dernière mise à jour : 2025). *Stratégie de l'intégration de l'IA dans l'administration publique 2021-2026*. https://www.quebec.ca/gouvernement/politiques-orientations/strategie-integration-ia-administration-publique-2021-2026

2 Gouvernement du Québec (dernière mise à jour : 2025). *Potentialités de l'IA dans l'administration publique*. https://www.quebec.ca/gouvernement/politiques-orientations/strategie-integration-ia-administration-publique-2021-2026/potentialites-ia-administration-publique

3 Données Québec (2025). *Portrait public des utilisations de l'IA dans l'administration publique québécoise*. https://www.donneesquebec.ca/recherche/dataset/portrait-public-des-utilisations-de-l-ia-dans-l-administration-publique-quebecoise

4 *Ibid.*

5 https://declarationmontreal-iaresponsable.com/

6 Marchildon, A., Jacob, S. et Marcoux, AM. (2021). Obvia. https://doi.org/10.61737/OXHA5372

Un récent sondage réalisé par NETendances (2025) indique que près de 45 % des répondants et des répondantes ne sont pas favorables à l'utilisation de l'IA par le gouvernement du Québec[7]. L'acceptabilité sociale de l'usage de l'IA dans les services publics est donc fragile. Une autre enquête de NETendances (2025) sur l'intelligence artificielle générative (IAg) concluait que « de façon générale, les internautes du Québec avaient certaines craintes liées à l'utilisation de l'intelligence artificielle, comme le risque pour leurs données personnelles, le manque de fiabilité ou encore des enjeux d'ordre éthiques » [8].

Enfin, dans les services publics, il importe de distinguer l'intelligence artificielle, les systèmes algorithmiques et les mécanismes d'automatisation. Bien que ces notions soient souvent regroupées dans le débat public, elles présentent des risques et des impacts distincts. Plusieurs enjeux abordés dans le présent mémoire concernent l'ensemble des systèmes automatisés de traitement de l'information et d'aide à la décision, qu'ils reposent ou non sur des techniques d'intelligence artificielle au sens strict.

Ce mémoire soutient que l'évaluation de l'utilisation de l'IA dans les services publics doit dépasser les seuls critères d'efficacité administrative. Elle doit également prendre en compte les impacts de toute nature sur l'accès aux services, la notion même de services publics, l'équité de traitement, la protection des droits fondamentaux et la confiance du public envers les institutions.

7 Académie de la transformation numérique (2025). *NETendances 2025 : Services gouvernementaux en ligne.* https://transformation-numerique.ulaval.ca/wp-content/uploads/2026/06/netendances25-services-gouvernementaux-en-ligne.pdf, p. 27

8 *Ibid.*

Section 1 - Fractures numériques : inégalités et exclusions face à la numérisation des services publics

Le recours à l'IA dans les services publics pour l'aide à la prise de décision ou pour le traitement des dossiers, s'ajoutant à la numérisation déjà bien amorcée de ceux-ci (procédures entièrement en ligne), transforme l'accès et la nature des services publics. Ces transformations ont pour risque de renforcer, voire d'amplifier les fractures[9] numériques préexistantes, qui se manifestent tant par des inégalités d'accès aux technologies, des inégalités de littératie numérique et des inégalités sociétales structurelles (systémiques). On identifie généralement **trois niveaux**[10] de fracture numérique. Le **premier** niveau correspond aux inégalités d'accès (au matériel et à la connectivité), alors que le **second** concerne les inégalités d'usage, c'est-à-dire la littératie et les compétences numériques. Le **troisième** niveau de fracture « réfère aux inégalités dans les avantages susceptibles d'être tirés de l'usage du numérique (bénéfices sociaux sur les plans de l'éducation, de l'emploi, de la santé, de la participation à la vie administrative et citoyenne, etc.) ». Ces différents niveaux de fracture sont étroitement interreliés et peuvent avoir une incidence importante sur l'accès à des services publics.

En plus de ces trois niveaux, certains écrits scientifiques identifient un **quatrième** niveau, portant sur les inégalités de représentativité dans les jeux de données et dans la conception des outils technologiques[11]. Par exemple, un groupe de population peut être sous-représenté dans certaines données en santé, ce qui entraîne des enjeux structurels quant à l'adéquation des types de services offerts pour répondre aux besoins de ce groupe sur le terrain. Dans le même ordre d'idée, un groupe de personnes qui serait surreprésenté dans les données en matière de justice, du fait d'un profilage racial par des forces de police, peut se voir ciblé davantage lorsqu'un service est automatisé par l'IA, amplifiant alors des injustices préexistantes.

Une **sous-représentation** ou une **surreprésentation** dans les données entraîne également des inégalités au niveau de la qualité et de la pérennité des services publics. En effet, lorsqu'un système d'IA est intégré à un service numérique afin d'anticiper les besoins futurs à partir des données de ses usagers, les prédictions produites reposent exclusivement sur les profils et les comportements des personnes qui utilisent déjà ce service[12]. Les besoins des non-usagers demeurent alors invisibles pour le système, ce qui risque de contribuer à reproduire ou à accentuer certaines inégalités, et donc à pérenniser une certaine invisibilité sociale pourtant connue et documentée. Ce quatrième niveau est étroitement associé à la question des biais algorithmiques, qui sera abordée plus en détail dans une section ultérieure (*voir section 3*).

Plusieurs facteurs peuvent influencer les niveaux de fractures numériques et, par conséquent, l'accès et la délivrance des services publics[13]. Ces facteurs de vulnérabilité numérique sont notamment : l'âge, la situation géographique, les compétences numériques, le revenu, le niveau d'éducation, le fait de vivre seul et le statut d'immigrant[14]. Les inégalités technologiques ou numériques sont fortement liées aux iniquités sociales préexistantes et les effets de leurs interactions viennent amplifier la marginalisation sociale et renforcer l'inadéquation des services publics par rapport aux besoins sur le terrain.

---

9 Jacob, S. et Brousseau, S. (2025). *Quand l'algorithme décide. L'état, l'IA et nous*, PUL.

10 Niveaux formulés par Brotcorne et Vendramin (2021), repris dans Hébert, V. et al. (2024). *La fracture numérique : contexte québécois, pistes d'action et perspectives internationales.* Rapport INRS. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/emploi-solidarite-sociale/publications-adm/rapport/RA_INRS_fracture_num.pdf

11 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

12 Gentelet, K., & Bahary-Dionne, A. (2021). Les angles morts des réponses technologiques à la Covid-19 : Des populations marginalisées invisibles. *Éthique publique, 23*(2). https://doi.org/10.4000/ethiquepublique.6441

13 Hébert, V. et al. (2024). *La fracture numérique : contexte québécois, pistes d'action et perspectives internationales.* Rapport INRS. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/emploi-solidarite-sociale/publications-adm/rapport/RA_INRS_fracture_num.pdf, p. 29

14 *Ibid.* p. 26

Ainsi, si l'introduction d'outils automatisés (formulaires interactifs, tri algorithmique des demandes, agents conversationnels, etc.) peut simplifier les démarches pour une partie de la population, elle peut, à l'inverse, **complexifier celles des publics en situation de vulnérabilité socioéconomique** :

- Difficulté à interagir efficacement avec des interfaces numériques et à comprendre l'information;
- Dépendance accrue à des intermédiaires (organismes communautaires, proches) avec les risques pour la protection de la vie privée et des renseignements personnels que peuvent entraîner les recours au soutien d'aidants numériques;
- Difficulté à comprendre les décisions automatisées, identifier les erreurs et les contester.

La transformation numérique des services publics produit des **inégalités d'accès différenciées, notamment selon les caractéristiques socioéconomiques des populations**. Ces inégalités conduisent à des formes d'**exclusion administrative**, où certaines personnes « renoncent à » avoir accès à des services ou ne sont pas en mesure de faire valoir leurs droits. Le cas du logiciel UNIR, récemment déployé par le ministère de l'Emploi et de la Solidarité sociale, est un exemple parlant de cette problématique (*voir section 3*).

Pour mitiger ces risques de discrimination et d'exclusion, il existe différentes **pratiques de conception inclusive**:

Ces pratiques de conception inclusive ne sont toutefois pas encore fortement intégrées dans les processus de développement des services publics numériques[16]. De plus, leur simple existence ne garantit pas une réelle inclusion. Ainsi, **lorsqu'une alternative hors ligne est offerte, celle-ci doit être accessible dans des conditions comparables à celles du service numérique**. Des délais de traitement plus longs, des coûts supplémentaires ou une disponibilité réduite peuvent constituer des obstacles importants pour les personnes qui y ont recours. Dans de telles situations, l'alternative hors ligne risque davantage de créer une filière de service de second ordre que de représenter une véritable mesure d'inclusion. Le maintien d'options analogues peut donc être considéré comme une pratique de conception inclusive seulement si ces options permettent un accès équitable aux mêmes services et permettent de jouir des mêmes droits.

La mise en place de telles **pratiques de conception inclusive** permettrait de répondre à plusieurs enjeux liés à l'utilisation de l'IA dans les services publics, dont la **confiance, la facilité d'usage et l'acceptabilité sociale.**

En somme, les risques associés à l'utilisation de l'IA dans les services publics ne se limitent pas aux enjeux technologiques ou techniques. Ils concernent directement l'égalité d'accès aux services et la capacité des citoyens à exercer leurs droits. Dans ce contexte, les fractures numériques doivent être considérées comme un risque systémique pouvant compromettre les objectifs mêmes de modernisation poursuivis par l'État. Une approche fondée sur l'inclusion numérique, sur le maintien d'alternatives non numériques fonctionnelles et sur la participation citoyenne apparaît donc essentielle pour limiter les effets d'exclusion et renforcer la confiance envers les services publics utilisant l'intelligence artificielle.

15 *Ibid.*, p. 32
16 *Ibid.*

Section 2 - Protection des renseignements personnels, droit à la vie privée et acceptabilité sociale

Lorsqu'il est question d'utilisation de l'IA ou d'algorithmes dans la prestation d'un service public, un enjeu central réside dans la protection des renseignements personnels des citoyens et des citoyennes ainsi que le respect de leur droit à la vie privée. Un projet gouvernemental qui illustre bien les multiples questionnements du public face à ces principes est le programme Service québécois d'identité numérique[17] (SQIN), soutenu par la *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (projet de loi n° 82), sanctionnée le 28 octobre 2025.

« Cette loi confie au ministre de la Cybersécurité et du Numérique la responsabilité de la gouvernance et de la gestion centralisée de l'identité numérique nationale, cette dernière étant un ensemble de moyens dont dispose l'État pour permettre à toute personne d'avoir un accès sécurisé aux prestations électroniques de services gouvernementales ainsi qu'un niveau de confiance élevé lors de ses interactions avec les organismes publics et dans la collectivité, notamment à l'aide d'attestations numériques gouvernementales. »[18]

Le SQIN vise à développer l'**identité numérique citoyenne**, c'est-à-dire « la représentation numérique d'une personne lui permettant de prouver son identité [...] [afin] de se connecter aux prestations électroniques de services gouvernementales et d'effectuer des démarches en ligne ou en personne »[19]. Dans une optique de modernisation de l'accès aux différents services gouvernementaux, ce projet et une multitude d'autres s'inscrivent dans la continuité de la stratégie de transformation numérique du gouvernement. Deux questions prioritaires demeurent : 1 le gouvernement prend-il toutes les mesures nécessaires pour assurer la sécurité des données des personnes et 2 les Québécois et les Québécoises sont-ils prêts à accepter ces nouvelles technologies?

1 Dans le premier cas, peu d'information est actuellement disponible sur le fonctionnement précis d'une éventuelle identité numérique citoyenne, sur le ou les prestataires de services qui seraient impliqués ou encore sur l'hébergement des données des usagers. Lors de l'étude du projet de loi n° 82, l'Obvia avait soulevé, dans un mémoire[20], des inquiétudes quant au manque d'information relative au rôle du secteur privé dans la constitution des infrastructures à la base de l'identité numérique nationale.

« **Pour des raisons de transparence et d'acceptabilité sociale**, il serait donc judicieux de clairement baliser et justifier le recours éventuel à la sous-traitance et aux partenariats publics-privés dans le projet de loi et de clarifier où seront hébergées les données gouvernementales et les attestations numériques gouvernementales. Pour des raisons d'analyse des **enjeux de sécurité et de vie privée**, il est important que l'architecture envisagée, ainsi que les protocoles d'authentification et d'échanges de données qui seront mis en place, soient détaillés afin de pouvoir être audités par des experts en sécurité et protection des données. La transparence sur ces aspects est un ingrédient nécessaire pour réaliser une étude des facteurs relatifs à la vie privée (EFVP) qui analyserait en amont les risques de vie privée liés au projet d'identité numérique, permettant d'intégrer adéquatement cette analyse dès la conception du système. »[21]

17 Gouvernement du Québec (dernière mise à jour : 2026). *Programme Service québécois d'identité numérique.* https://www.quebec.ca/gouvernement/identite-numerique/programme-service-quebecois-identite-numerique

18 Assemblée Nationale du Québec (2024). *Projet de loi no 82 - Loi concernant l'identité numérique nationale et modifiant d'autres dispositions.* https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2025/2025C26F.PDF

19 Gouvernement du Québec (dernière mise à jour : 2026). *op.cit.*

20 Loiseau, H., Caron, D.J., Gambs, S. et Brousseau, S. (2025). *Pour une identité numérique québécoise au service des citoyens : enjeux et recommandations.* Obvia. Mémoire présenté à la Commission des finances publiques lors des consultations particulières et auditions publiques sur le projet de loi 82, Loi concernant l'identité numérique nationale et modifiant d'autres dispositions. https://doi.org/10.61737/ZFCY4930

21 *Ibid.*, p.10

L'hébergement des données et l'origine des fournisseurs de services sont d'une importance capitale pour la protection des renseignements citoyens, dont les données sensibles, notamment en raison de lois extraterritoriales qui permettent à des acteurs étrangers de mettre la main sur ces données. En particulier, le **Cloud Act** (*Clarifying Lawful Overseas Use of Data*) permet au gouvernement américain de contraindre des entreprises dont le siège social est situé ou affilié aux États-Unis ou qui exercent simplement des activités sur le sol américain à lui communiquer les données qu'elles détiennent, y compris des données à caractère personnel qui ne sont pas hébergées sur le sol américain[22]. Il n'est pas ici question d'actes illégaux, comme des cyberattaques par des entités malveillantes, mais bien de **recours réguliers entièrement légaux pour avoir accès à des données québécoises, même si elles sont hébergées au Québec ou au Canada**.

Il y a donc un impératif de **prudence** par rapport aux contrats qui sont octroyés à des entreprises privées, surtout qu'en raison des capacités gouvernementales (ressources humaines et technologiques), il est bien souvent nécessaire d'avoir recours à de l'expertise externe. Cette préoccupation face à la protection des renseignements personnels a été mise en lumière par le déploiement récent du Dossier santé numérique (DSN) au Québec, puisque le logiciel utilisé est fourni par l'entreprise américaine Epic Systems et qu'il est question de données médicales et sensibles. Il y a ici une certaine incohérence entre les objectifs formulés par le gouvernement du Québec en matière de **souveraineté numérique** et la réalité sur le terrain. En plus de la Loi[23] qui mentionne le renforcement de la souveraineté numérique, *l'Énoncé de politique de souveraineté numérique et d'approvisionnement en technologie de l'information*[24] du ministère de la Cybersécurité et du Numérique vient consolider les ambitions du gouvernement en matière d'émancipation de certaines dépendances technologiques. Or, malgré les risques, le gouvernement continue d'octroyer des contrats à des entreprises étrangères (surtout américaines)[25], ce qui fragilise la sécurité des données des citoyens et des citoyennes.

Enfin, l'utilisation d'algorithmes et d'IA dans la prestation de services publics engendre des risques par rapport à la **confidentialité** et au **respect de la vie privée** des usagers et usagères. Par exemple, le recours à une identité numérique pour l'accès à différents services laisse des empreintes électroniques qui sont susceptibles d'être collectées, stockées et exploitées de manière automatique[26]. La centralisation de ces données ouvre la porte à du croisement appuyé par l'IA et à la génération de nouvelles données « **qui peuvent mener à un profilage précis et à des risques de surveillance. Cela ouvre ainsi la possibilité pour le gouvernement d'utiliser ces données pour catégoriser les citoyens par rapport à leurs comportements en termes de santé, de mobilité ou de gestion financière** »[27]. Ainsi, le gouvernement a la responsabilité d'assurer que tout service numérisé, qu'il intègre ou non un dispositif d'IA, ne permette pas la collecte ou le croisement des données à des fins non explicitées dans la loi ou qui vont à l'encontre du droit à la vie privée.

---

22 Placca, M., Loiseau, H. et Poisson, E. (2026). *Construire la souveraineté numérique au Québec : état de la littérature et synthèse de colloque*. Obvia. https://doi.org/10.61737/AQDK8798, p.19

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

24 Gouvernement du Québec, ministère de la Cybersécurité et du Numérique (2026). *Énoncé de politique de souveraineté numérique et d'approvisionnement en technologie de l'information*. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/Enonce_politique_souverainete_numerique.pdf

25 Par exemple, le MCN a octroyé plus de 400 millions de dollars en contrats publics à Amazon Web Services. Voir : Roy, J-H. (2025, janvier). *Plus de 400 millions en contrats publics à Amazon*. La Presse. https://www.lapresse.ca/actualites/2025-01-24/amazon-web-services/plus-de-400-millions-en-contrats-publics-a-amazon.php

26 Loiseau, H., Caron, D.J., Gambs, S. et Brousseau, S. (2025). *op.cit.,* p.10

27 *Ibid.*

2 En ce qui concerne l'acceptabilité sociale, des études récentes brossent un portrait mitigé. Deux facteurs clés semblent toutefois se dégager pour favoriser l'adoption des nouveaux outils numériques par les individus : la réalisation de certaines **conditions** entourant leur déploiement et l'augmentation du niveau de **confiance** accordée aux autorités gouvernementales.

Dans un premier temps, selon une enquête menée auprès de 2 020 répondants sur la confiance et l'acceptabilité sociale dans l'usage de l'identité numérique au Québec, « seuls 12,3 % se sont initialement montrés totalement ouverts à l'utilisation de l'identité numérique alors que près du double, soit 23,1 %, ont signifié n'être pas du tout ouverts à l'utilisation de celle-ci. La plus grande proportion des répondants (64,7 %) se sont dits ouverts, mais à certaines conditions »[28]. Lorsque les chercheurs ont ensuite présenté des conditions d'implantation possibles, le niveau d'ouverture des participants a augmenté : **après deux rondes d'ajout de conditions, la proportion des répondants se disant ouverts à l'utilisation de l'identité numérique passe à près de 95%**. L'encadré qui suit présente les conditions qui augmentent le plus l'adhésion au projet de SQIN, en ordre d'importance accordée par les participants.

Conditions qui favorisent l'ouverture à l'identité numérique[29]

1. Implantation de meilleurs systèmes de sécurité
2. Réduction des délais pour accéder aux services publics
3. Limitation du nombre d'endroits où sont détenus les renseignements personnels
4. Facilitation de la communication avec le gouvernement du Québec pour accéder aux services gouvernementaux
5. Accès à tous les services du gouvernement du Québec à partir d'un seul endroit

Dans un deuxième temps, la **confiance** accordée par les citoyens et les citoyennes aux projets comme le DSN et le SQIN est centrale pour leur réussite. **Un premier frein** à cette confiance se perçoit dans la **méconnaissance ou l'incompréhension du fonctionnement** de ces nouvelles initiatives. Comme le révèle une étude ayant fait appel à des groupes de discussion avec des membres du public[30], les citoyens et les citoyennes sont trop peu informés ou sensibilisés quant aux tenants et aboutissants des projets, ce qui réduit leur potentiel de consentement à les utiliser. Le manque de connaissance envers les projets mine également la confiance du public, puisque **les bénéfices ne sont pas connus**. Par rapport au SQIN, « les études montrent que lorsque le public est mieux informé du fonctionnement et des avantages anticipés du SQIN, le niveau de confiance envers le projet augmente »[31].

La perception de la capacité gouvernementale à piloter adéquatement ces projets constitue **un deuxième frein** à la confiance citoyenne envers les projets de transformation numérique. Selon les études menées auprès des membres du public, il existe un écart entre la perception de la **volonté** et de la **capacité** du gouvernement à mener à bien des initiatives numériques[32]. Les personnes ont généralement confiance envers la volonté du gouvernement de protéger leurs données et de gérer de manière responsable ces renseignements, mais elles doutent de la capacité du gouvernement à le faire, que ce soit par un manque d'expertise à l'interne ou d'infrastructures appropriées. « Les raisons évoquées pour cette remise en question de la capacité concernent les investissements qui ne sont pas jugés suffisants, ainsi que les «échecs» de projets gouvernementaux antérieurs »[33].

28 Caron, D.J., Lamarche, P.-O., Nicolini, V. et Prud'homme, A. (2025). *Enquête sur la confiance et l'acceptabilité sociale dans l'usage de l'identité numérique au Québec.* Obvia.https://doi.org/10.61737/UXSD7760, p. 14
29 *Ibid.*, p. 16
30 Caron, D.J., Lamarche, P.-O. et Nicolini, V. (2025). *La confiance comme levier pour le partage des renseignements personnels et de santé : perspectives citoyennes.* Obvia. https://doi.org/10.61737/XOZU2116
31 Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique. (2025). *Dans l›oeil de l›Obvia - La confiance envers l'identité numérique québécoise : état des lieux.* Obvia. https://doi.org/10.61737/BPDA9511
32 Caron, D.J., Lamarche, P.-O. et Nicolini, V. (2025). *op.cit.,* p. 17
33 *Ibid.*, p. 20

À l'inverse, les personnes sondées accordent leur confiance plus facilement aux capacités du **secteur privé** de déployer de tels projets, mais elles remettent en question la bonne volonté de ces acteurs, puisque le privé est associé à la volonté de faire un profit[34]. Ainsi, avec l'exemple du SQIN, les participants aux études souhaitent que le projet soit géré par le gouvernement, mais que celui-ci investisse stratégiquement, d'une part pour faire affaire avec des entreprises compétentes, d'autre part pour rendre les salaires plus compétitifs dans la fonction publique et ainsi attirer des experts au sein même du gouvernement[35].

Un troisième frein à la confiance est l'absence d'une véritable **démarche inclusive et consultative** sur l'usage de l'IA dans les services publics mobilisant les personnes citoyennes. En octobre 2024, le gouvernement du Québec avait annoncé la tenue, sur leur plateforme en ligne (avec un délai de moins de 30 jours), d'une consultation publique autour de l'utilisation de l'identité numérique et de l'intelligence artificielle[36] dans les services gouvernementaux, qui aurait été suivie d'un volet présentiel sous la forme de groupe de discussion. Cependant, cette consultation a été annulée.

Constatant ce manque de démarches consultatives sur l'utilisation de l'IA dans les services publics, l'Obvia et l'organisme Communautique[37] ont réalisé une étude exploratoire pour comprendre comment les personnes citoyennes souhaitaient être consultées, mais surtout mobilisées pour participer à la prise de décision sur les questions d'utilisation de l'IA au sein de l'appareil gouvernemental. L'étude identifie plusieurs conditions pour assurer qu'un dialogue citoyen de qualité et une participation informée sur les enjeux locaux soient mis en place[38] :

- Renforcer l'information citoyenne autour de l'IA (fonctionnement, effets, etc.);
- Créer des espaces formels et pérennes de dialogue sur les déploiements d'outils d'IA dans les services publics;
- Favoriser la diversité des formats de participation afin d'inclure tous les profils des personnes citoyennes;
- Offrir une participation à partir de cas concrets (pas de consultation sur des enjeux hypothétiques et sans lien avec les services publics);
- Reconnaître la diversité des savoirs et la pertinence des expertises terrain en ce qui concerne l'évaluation des besoins et la pertinence de recourir à l'IA.

En plus de favoriser la confiance et l'acceptabilité sociale, de telles démarches participatives permettent d'améliorer la pertinence du service offert et de corriger les biais anticipés et réels envers certains groupes ou individus pour renforcer l'équité. Cela permet d'inclure les personnes citoyennes dans une gouvernance démocratique des outils d'IA.

34 *Ibid.*, p. 18
35 Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique. (2025). op.cit.
36 Gouvernement du Québec (2024). *Identité numérique et intelligence artificielle : le gouvernement du Québec invite la population à participer à une consultation publique*. https://www.quebec.ca/nouvelles/actualites/details/identite-numerique-et-intelligence-artificielle-le-gouvernement-du-quebec-invite-la-population-a-participer-a-une-consultation-publique-58615
37 https://www.communautique.quebec/
38 Gentelet, K., Peñalosa, R., Aigoin, M., Dion, M.-C., et Hajjsleiman, J. (2025). *Imaginer un dialogue citoyen sur l'IA dans les services publics: recommandations pour une gouvernance fondée sur la transparence et la confiance*. Obvia. https://doi.org/10.61737/LPLW5969, p. 27

Section 3 - L'automatisation des services avec l'IA : équité, biais et contrôle humain

Dans la quête d'efficience et de réduction des coûts de l'administration publique, des systèmes d'IA peuvent être utilisés pour automatiser, en totalité ou en partie, certains processus décisionnels. Tel que mentionné précédemment, la mise en place du système UNIR au sein du ministère de l'Emploi et de la Solidarité sociale est un exemple récent de cette tendance. En raison de ses ratés, cette initiative a fait l'objet d'un reportage à l'émission *Enquête* en mars 2026. À la suite de ces révélations et à la demande d'organisations de la société civile, dont plusieurs soutiennent les personnes citoyennes dans leurs démarches administratives, l'Obvia a organisé un webinaire pour analyser les impacts que ce système sur les bénéficiaires[39].

Le système UNIR repose sur la numérisation complète des dossiers, leur gestion électronique et l'automatisation de leur traitement. **Les dossiers ne sont plus suivis par un agent attitré**, puisqu'un système algorithmique attribue désormais les tâches aux agents disponibles à l'échelle du Québec en fonction de priorités définies automatiquement. Cette logique centralisée et automatisée marque un passage important d'un accompagnement personnalisé vers une gestion standardisée et mécanique des demandes.

Il s'agit d'un changement majeur pour les prestataires de services publics, plusieurs étant déjà en situation de vulnérabilité. Par exemple, la disparition du suivi personnalisé oblige les personnes à répéter leur situation à plusieurs intervenants, ce qui peut être vécu comme **déshumanisant,** difficile et socialement stigmatisant. Des problèmes de délais, d'erreurs administratives ou de perte de documents sont également signalés, ce qui peut avoir des conséquences importantes sur le bien-être social, physique et mental des victimes d'erreurs commises par l'algorithme. On doute ainsi de « la capacité des systèmes algorithmiques à pouvoir s'adapter à des situations imprévues ou à exercer le degré de discernement dont l'humain est capable face à des situations sociales complexes et nuancées »[40]. L'IA peut entraîner une dépersonnalisation de la relation entre l'administration et la personne qui reçoit le service. À terme, il convient de questionner le bien-fondé des services publics censés soutenir des populations en situation de vulnérabilité et pallier une certaine précarité sociale.

Les erreurs de traitement commises par un algorithme peuvent découler de la complexité du dossier à traiter, mais aussi de la présence de **biais algorithmiques** dans la programmation du système. De tels défauts du système apparaissent lorsque les données sur lesquelles celui-ci est entraîné reflètent elles-mêmes des biais sociétaux. Ces biais sont difficiles à éviter, considérant que les données reflètent les dynamiques sociétales, où persistent des inégalités et des préjugés. « En effet, en analysant de grands ensembles de données, les algorithmes privilégient les groupes majoritaires et diluent la voix des groupes minoritaires »[41].

Certes, il est possible d'atténuer certains écueils en travaillant à partir de données mieux catégorisées, mais cela ne règle pas les enjeux plus profonds générés par les représentations sociétales biaisées des personnes en situation de vulnérabilité (par exemple que ces personnes profiteraient du système et devraient être surveillées). D'autres enjeux demeurent également, comme les injustices épistémologiques liées à la représentation des systèmes de connaissances non occidentaux, notamment ceux des Premiers Peuples[42]. La numérisation des services ne signifie pas la réduction des iniquités systémiques, et, au contraire, peut les amplifier. Finalement, les **solutions pour « débiaiser »** des algorithmes ne sont généralement pas simples à trouver en présence de parcours complexes, d'autant plus qu'il est difficile de corriger une situation d'injustice découlant d'une décision algorithmique.

39 Obvia (2026). *Confier l'aide sociale à un algorithme : regard sur le programme UNIR*. https://www.obvia.ca/ressources/confier-laide-sociale-a-un-algorithme-regard-sur-le-programme-unir

40 Jacob, S., et Brousseau, S. (2025). *Quand l'algorithme décide : l'État, l'IA et nous*. Presses de l'Université Laval, p. 3

41 *Ibid.*, p. 47

42 Gentelet, K., & Bahary-Dionne, A. (2021). Stratégies des Premiers Peuples au Canada concernant les données numériques : décolonisation et souveraineté. *tic&société, 15*(1), 189–208. https://doi.org/10.4000/ticetsociete.6063

Au-delà des biais au sein même d'un système algorithmique, le recours à un outil d'aide à la décision peut également induire un **biais d'automatisation** chez la personne qui doit prendre la décision finale. C'est ce qui s'est produit à Immigration, Réfugiés et Citoyenneté Canada (IRCC) avec leur dispositif surnommé « Chinook »[43], dont l'intégration aurait causé une augmentation des demandes refusées, particulièrement pour les permis d'études. L'une des fonctionnalités de ce système est de trier les demandes selon un certain niveau de risque, pouvant être basé sur une prédiction de la probabilité que la personne commette des infractions ou dépasse le temps alloué par le visa. Les agents et les agentes devant traiter les demandes sont ainsi informés du niveau de risque identifié par Chinook, sans savoir sur quelle(s) base(s) un risque élevé aurait été identifié, ni par rapport à quelle section de la demande. Ce procédé peut induire un biais d'automatisation, défini comme **un excès de confiance accordée à un système d'assistance à la décision, entraînant une influence de ce système sur la décision et le jugement de l'humain[44].**

Afin de limiter les biais d'automatisation, il est primordial que les gestionnaires de la fonction publique disposent d'une formation afin de comprendre le fonctionnement des algorithmes, leurs objectifs ainsi que leurs limites, de manière à pouvoir exercer un jugement critique éclairé. Cet enjeu relève directement de la **littératie numérique et d'IA**. Il nécessite une formation adéquate permettant de développer les connaissances requises et de sensibiliser les utilisateurs aux risques et répercussions associés à l'IA sur les droits des personnes.

En s'appuyant sur ces systèmes pour automatiser des décisions et traiter les dossiers plus rapidement**, les risques de biais, de discrimination et d'atteinte aux droits fondamentaux** sont bien présents. Il existe également un risque de **perte de contrôle** sur les processus décisionnels. Le contrôle a une incidence déterminante sur la confiance envers le bien-fondé des services publics, de la solidarité sociale et de la démocratie. Les dispositifs d'IA doivent rester dans une boucle de transparence, de contrôle et d'imputabilité, que ce soit lors de leur développement, leur utilisation, leur gouvernance ou leur évaluation. Maintenir cette boucle d'imputabilité dans les processus de décision ou de traitements automatisés est essentiel. Cela ne se limite pas à disposer des compétences nécessaires pour comprendre le fonctionnement des systèmes ni à mettre en place des mécanismes clairs pour corriger leurs erreurs[45] : c'est l'ensemble du système démocratique qui doit être mobilisé.

43 Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique. (2024). *Dans l'œil de l'Obvia - Décision automatisée et immigration : enjeux et leçons pour le secteur public*. Obvia. https://doi.org/10.61737/TFCE3938

44 *Ibid.*

45 *Ibid.*

Conclusion

L'intégration de l'intelligence artificielle (IA) au sein des services publics québécois ouvre des perspectives réelles d'amélioration de l'efficience de l'État. Toutefois, les éléments présentés dans ce mémoire montrent que cette intégration ne peut se limiter à des considérations d'efficacité et de performance administratives. L'IA dans les services publics comporte des risques réels touchant directement l'accès aux services, l'exercice des droits, la protection de la vie privée, l'équité de traitement et la confiance envers les institutions publiques.

Les risques recensés sont multiples et interreliés. La transformation numérique et l'automatisation des services peuvent accentuer les fractures numériques existantes, particulièrement chez les personnes en situation de vulnérabilité, et ainsi créer de nouvelles formes d'exclusion administrative. L'utilisation croissante de systèmes algorithmiques soulève également des préoccupations importantes quant à la protection des renseignements personnels et au respect de la vie privée, notamment lorsque des données sensibles sont confiées à des infrastructures ou à des fournisseurs externes.

Par ailleurs, les biais algorithmiques reproduisent, voire amplifient, des inégalités et des discriminations déjà présentes dans la société. Les mécanismes d'automatisation, quant à eux, peuvent contribuer à une dépersonnalisation de la relation entre l'administration publique et les personnes citoyennes, particulièrement lorsque des décisions ou le traitement de dossiers complexes sont standardisés. Le manque de transparence de certains systèmes et les difficultés à comprendre, contester ou corriger des décisions automatisées soulèvent par ailleurs des enjeux importants de reddition de comptes, d'imputabilité et de contrôle démocratique.

Les travaux cités montrent néanmoins que ces risques ne sont pas inévitables. Leur atténuation passe par l'adoption de principes de prudence, d'équité, de transparence et de participation citoyenne tout au long du cycle de vie des systèmes. Cela implique notamment de renforcer les mécanismes de gouvernance, de maintenir des alternatives non numériques accessibles et équitables, de protéger rigoureusement les renseignements personnels, de former adéquatement les acteurs publics et de créer des espaces pérennes de dialogue avec les personnes citoyennes.

En définitive, la question n'est donc pas de déterminer si l'administration publique doit utiliser ou non l'intelligence artificielle, mais plutôt dans quelles conditions elle peut le faire de manière légitime, responsable et démocratique.

obvia

obvia.ca