

DE : Monsieur Gilles Bélanger
Ministre de la Cybersécurité et du Numérique

Le 9 décembre 2025

TITRE : Énoncé de politique de souveraineté numérique et d'approvisionnement en technologie de l'information (TI)

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

Désormais au cœur du fonctionnement de l'État et de la prestation des services publics, l'environnement numérique est en profonde transformation et pose des défis stratégiques majeurs.

Les données gouvernementales, celles des citoyens et celles des entreprises, constituent des actifs essentiels dont la protection, la localisation et la gouvernance ne peuvent pas être laissées au hasard et doivent être encadrés.

Dans un contexte où la compétitivité économique, la sécurité nationale et la confiance citoyenne dépendent de plus en plus de la capacité d'un État à maîtriser ses actifs numériques, il devient essentiel pour le Québec de clarifier sa position en matière de souveraineté numérique.

Souveraineté numérique

La souveraineté numérique réfère à la capacité d'un État à exercer un contrôle autonome de ses infrastructures (serveurs et réseaux), de ses technologies et de ses données. Elle englobe la gestion sécurisée des informations, la protection des données personnelles et la confidentialité des échanges numériques.

Elle vise à préserver l'indépendance stratégique de l'État et à soutenir sa transformation numérique de manière fiable et durable.

Encadrements existants

Le gouvernement a déjà adopté et publié certains documents qui prévoient des orientations en matière de souveraineté numérique.

C'est le cas de la *Stratégie gouvernementale des marchés publics*, publiée en février 2022, qui vise notamment à favoriser « l'achat québécois », y compris pour les approvisionnements en TI.

La *Stratégie gouvernementale de cybersécurité et du numérique 2024-2028*, adoptée en juillet 2024, dont les trois axes portent sur le renforcement de la cybersécurité de l'administration publique, l'accélération de sa transformation numérique et le

développement d'infrastructures technologiques pérennes et sécuritaires, présente également des assises complémentaires.

Enfin, la *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (2025, chapitre 26), sanctionnée le 28 octobre 2025, prévoit que le ministre peut développer des moyens visant à renforcer la souveraineté numérique en matière de gouvernance et de gestion des ressources informationnelles. Cette loi établit également que, dorénavant, le ministre de la Cybersécurité et du Numérique a la responsabilité de développer et de soumettre au gouvernement une vision globale des infrastructures et des services de télécommunications jugés utiles ou essentiels pour la conduite des affaires de l'État¹.

2- Raison d'être de l'intervention

Si, d'une part, le Québec est confronté à un défi qui nécessite d'accroître le contrôle sur ses actifs technologiques, il existe d'autre part un besoin essentiel de confirmer aux citoyens sa capacité à assurer la gouvernance numérique de l'État et d'augmenter ses moyens pour agir en faveur de ses propres intérêts en la matière.

Le gouvernement du Québec ne dispose pas d'orientations spécifiques et politiquement affirmées encadrant la souveraineté numérique et les pratiques d'acquisition de solutions technologiques.

L'absence d'un positionnement politique structuré sur la souveraineté numérique limite donc la capacité du gouvernement du Québec à affirmer ses priorités et à se positionner dans un environnement numérique marqué par des rapports de force technologiques de plus en plus déterminants.

Il est capital que le gouvernement du Québec assume son leadership en matière de souveraineté numérique, d'autant plus que le Québec dispose d'atouts significatifs soutenant la mise en place d'une stratégie ambitieuse en la matière.

3- Objectifs poursuivis

En établissement des orientations clés en matière de gouvernance et de protection des données, d'innovations technologiques, de contrôle des infrastructures et d'indépendance numérique, il sera possible de diriger l'action gouvernementale en matière de souveraineté numérique pour protéger l'autonomie de l'État en ces matières. L'objectif est d'établir la base sur laquelle pourront ensuite être élaborées une politique et des initiatives ciblées, de manière progressive, maîtrisée et en collaboration avec les acteurs gouvernementaux concernés.

Il est également visé de renforcer l'intégrité des services numériques, d'appuyer l'autonomie technologique du Québec et de soutenir la fiabilité et la durabilité des services essentiels pour l'État et les citoyens.

¹ L'article 3 de *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (2025, chapitre 26) introduit l'article 5.2 à la *Loi sur le ministère de la Cybersécurité et du Numérique* (chapitre M-17.1.1)

4- Proposition

L'Énoncé, qui serait rendu public, propose de définir le socle stratégique qui servira de point d'ancrage pour définir les priorités en vue de l'organisation de la souveraineté numérique du Québec.

Concrètement, huit orientations reposant sur deux objectifs centraux sont proposées pour guider les actions du gouvernement afin que le Québec puisse structurer une gouvernance cohérente de ses acquisitions et de ses projets technologiques souverains, maîtriser ses technologies clés, renforcer la sécurité de ses infrastructures critiques et de ses données sensibles et pour soutenir le développement de l'expertise locale.

Objectif 1. Accroître la souveraineté numérique du Québec

1- Favoriser l'hébergement souverain des données au sein du Nuage gouvernemental du Québec (NGQ) et dans les centres de traitement informatique (CTI)

Accélérer l'expansion et l'évolution du NGQ en diversifiant les services offerts permettra l'intégration progressive des systèmes et données des organismes publics et favorisera l'hébergement souverain des données en assurant que les informations sensibles demeurent sous juridiction québécoise, dans des environnements contrôlés localement. Cette approche réduit la dépendance à l'égard de fournisseurs externes, améliore le contrôle sur les accès, la sécurité et la résilience des infrastructures, et garantit que les données essentielles à la mission de l'État sont protégées selon ses propres lois.

L'utilisation accrue des CTI détenus par les gouvernements du Québec ou du Canada ou encore par des entreprises québécoises ou canadiennes est une mesure complémentaire assurant également l'intégrité, la sécurité et la confidentialité des données. Ce faisant, les données des Québécois détenues ou gérées par l'administration publique sont localisées en sol québécois ou canadien, inaccessibles à de tiers étrangers.

2- Assurer le contrôle des données via des centres de données sous juridiction québécoise

Le Québec se distingue par des atouts stratégiques qui en font un emplacement privilégié pour le développement d'infrastructures technologiques souveraines, tel que les centres de données souverains. Portée par la démocratisation de l'intelligence artificielle (IA), la demande mondiale pour ce type d'infrastructure croît de manière exponentielle.

En plus de permettre au Québec de développer sa capacité à allier son hydro-électricité, une énergie propre, stable et abordable, à une gouvernance numérique indépendante, ce qui devrait contribuer à attirer des investissements et la création d'emplois au Québec, cette opportunité permettra de renforcer la protection des données sensibles de l'État en sol québécois, tout en soutenant la recherche et en réduisant la dépendance aux fournisseurs mondiaux d'infonuagique à grande échelle.

3- *Renforcer l'utilisation du logiciel libre et soutenir la création de solutions sur mesure*

Le logiciel libre est un des leviers essentiels pour développer la souveraineté numérique. Il offre une transparence accrue, une maîtrise complète du code et une réduction de la dépendance envers des fournisseurs uniques, ce qui améliore le contrôle de l'État sur son écosystème numérique.

En parallèle, le développement de solutions sur mesure doit être favorisé lorsque, dans certains cas, des changements trop importants sont nécessaires pour adapter les outils de type progiciel aux besoins spécifiques du gouvernement. L'IA offre d'ailleurs des opportunités pour accélérer ce type de développement personnalisé et permet d'accroître l'agilité technologique, tout en stimulant l'expertise locale. En effet, l'IA permet d'assister les développeurs et les programmeurs dans la création, l'évolution et l'entretien des actifs numériques. Elle peut notamment documenter le code, identifier les failles et suggérer les correctifs à apporter, en les expliquant, afin de permettre aux entreprises d'enrichir leur expertise.

Ensemble, ces approches favoriseront une plus grande autonomie stratégique et renforceront la résilience du numérique public.

Par ailleurs, le Québec dispose d'une occasion stratégique de se positionner comme leader en matière de logiciel libre en misant sur la collaboration entre acteurs publics², parapublics et internationaux³.

4- *Maximiser l'utilisation de la Plateforme de développement moderne (PDM)*

La PDM est un environnement intégré que développera le gouvernement du Québec pour standardiser et moderniser le développement des applications et services numériques, notamment les pratiques de cybersécurité associées. Elle vise à accroître l'agilité, la réutilisation des composantes logicielles, la sécurité et la qualité des systèmes, tout en favorisant l'innovation et la collaboration entre les équipes de TI gouvernementales.

Dans une perspective de souveraineté numérique, l'utilisation de la PDM permettra de mieux contrôler le cycle de vie des applications, d'assurer la sécurité des données et de développer des solutions adaptées aux besoins spécifiques de l'État.

Maximiser l'utilisation de la PDM centralisera davantage le développement des logiciels et applications critiques, en assurera un contrôle opérationnel direct et en simplifiera la maintenance.

² Le MCN est signataire, pour le Québec, de l'Entente de collaboration canadienne en matière de cybersécurité.

³ Ce type de partenariat est bien représenté par l'implantation de la technologie souveraine et logiciel libre X-Road auquel a accès le MCN depuis son adhésion comme partenaire à la *Nordic Institute of Interoperability Solutions* (NIIS). Depuis le 20 novembre 2024, le MCN est partenaire de la NIIS aux côtés de l'Estonie, de la Finlande, de l'Islande et de l'Ukraine.

5- S'inspirer des meilleures pratiques internationales en matière d'encadrement TI

Dans un contexte d'hégémonie croissante de certaines entreprises sur le marché numérique mondial, plusieurs États ont encadré leurs TI par des lois et directives visant à renforcer la cybersécurité et la gouvernance numérique. Il est proposé que le Québec se penche sur certaines pratiques internationales pour s'en inspirer.

Cela dit, toute initiative de ce type sera mise en œuvre dans le respect de la législation en vigueur, après consultation des autorités compétentes et en alignement avec les priorités de l'État, afin de préserver de manière responsable le contrôle des infrastructures, des données et des capacités d'innovation du Québec.

Objectif 2. Maximiser les retombées économiques des investissements de l'État en TI

6- Exploiter pleinement les marges de manœuvre disponibles au sein du cadre normatif en gestion contractuelle

En intégrant des clauses à portée stratégique dans les contrats à conclure avec des fournisseurs l'État pourra mieux encadrer ses acquisitions en TI. Cette approche favorisera la sélection de solutions conformes aux objectifs de souveraineté numérique, notamment en matière de contrôle des données et d'autonomie technologique. Elle favorisera également la diversification des sources d'approvisionnement, le soutien au développement de solutions locales et un approvisionnement plus flexible et plus résilient.

Toujours dans le respect des règles et procédures établies, l'application de mesures pour ajuster certains contrats pourra être envisagée, en fonction des besoins stratégiques ou des risques identifiés, notamment pour consolider la sécurité des données.

7- Bâtir une expertise et une capacité numérique locale forte

Le renforcement d'une expertise et d'une capacité numérique locale permettra d'accroître la résilience des services publics, de soutenir la compétitivité économique et d'assurer la maîtrise stratégique des technologies clés.

Pour y parvenir, il est essentiel d'investir dans la formation et le perfectionnement en matière de compétences numériques. Il conviendra également de soutenir l'innovation et de favoriser des partenariats stratégiques entre le gouvernement et l'industrie numérique québécoise.

Ces mesures permettront de consolider l'expertise locale pour favoriser l'autonomie du Québec en matière de développement TI et de gestion d'infrastructures numériques.

8- Préserver les investissements majeurs en TI au Québec

Certaines entreprises étrangères en TI exercent des activités au Québec, lesquelles ont des retombées économiques importantes et positives pour l'État. Préserver les

investissements majeurs faits en TI, y compris ceux provenant de l'étranger, contribuera à la souveraineté numérique en consolidant des capacités technologiques essentielles et en soutenant la disponibilité de services clés sur le territoire.

En maintenant ces investissements, le Québec s'assurera d'un écosystème technologique performant sur son territoire : les entreprises renforcent leurs compétences, forment davantage de spécialistes et développent des solutions davantage adaptées aux besoins du Québec. À terme, cela se traduira par une offre de fournisseurs plus diversifiée, mieux outillée pour répondre aux différents besoins gouvernementaux.

5- Autres options

Dans un contexte où les technologies évoluent rapidement, ne pas encadrer la souveraineté numérique revient à exposer l'État à des incompatibilités technologiques et à des risques systémiques.

Proposer une politique formelle engageant immédiatement l'ensemble de l'État dans des orientations prescriptives et des obligations opérationnelles a été envisagé. Toutefois, cette approche présentait le risque d'adopter une politique précipitée et inadaptée, dans un contexte où la transformation numérique redéfinit profondément les façons de gouverner. Dès lors, il devenait essentiel de favoriser, dans un premier temps, une concertation étroite avec l'ensemble des acteurs concernés.

6- Évaluation intégrée des incidences

Au niveau de la gouvernance numérique

Les organismes publics pourront compter sur des orientations clés en matière de gouvernance et de protection des données, d'innovations technologiques, de contrôle des infrastructures et d'indépendance numérique en matière de souveraineté numérique.

7- Consultation entre les ministères et avec d'autres parties prenantes

Les membres du Comité de gouvernance en ressources informationnelles (CGRI), présidé par le dirigeant principal de l'information et réunissant tous les dirigeants de l'information de la fonction publique québécoise, ont été consultés. Plus particulièrement, le Comité aviseur du CGRI a été mis à contribution pour commenter la proposition d'Énoncé.

L'Énoncé a également fait l'objet de présentations auprès du Secrétariat du Conseil du trésor, du ministère des Finances du Québec, du ministère de l'Économie, de l'Innovation et de l'Énergie (MEIE) ainsi que du Comité d'experts constitué par le ministre de la Cybersécurité et du Numérique.

Le MEIE, le ministère des Relations internationales et de la Francophonie, la Commission d'accès à l'information, Santé Québec et Investissement Québec ont formulé des commentaires lesquels ont été pris en considération. Les commentaires, recommandations et observations recueillis au cours de ces démarches ont permis de bonifier la présente proposition.

8- Mise en œuvre, suivi et évaluation

L'adoption des orientations présentées dans l'Énoncé constituera l'assise de l'élaboration d'une politique gouvernementale en matière de souveraineté numérique et d'approvisionnement en TI. Elle permettra d'établir, à la suite de consultations auprès de différents acteurs gouvernementaux et en collaboration, des orientations claires et cohérentes avec les priorités stratégiques du gouvernement, puis de définir, planifier et mettre en œuvre des initiatives concrètes visant à renforcer l'autonomie numérique de l'État.

9- Implications financières

L'adoption du présent Énoncé ne nécessite aucune somme.

10- Analyse comparative

Les différences entre les cadres juridiques internationaux en matière d'accès aux données posent des défis majeurs pour la protection de la vie privée et la souveraineté numérique des États. Plusieurs pays ont individuellement entrepris des initiatives importantes en la matière, notamment la France, l'Allemagne, la Finlande, le Royaume-Uni, l'Australie et l'Estonie.

D'ailleurs, une analyse publiée en 2024⁴ prévoit que 82 % des gouvernements de l'Asie-Pacifique intensifieront dans les prochaines années leurs investissements dans la poursuite de leur souveraineté numérique, alors que ce sera le cas de 64 % des gouvernements en Amérique du Nord et de 58 % de ceux d'Europe.

La préoccupation d'établir une souveraineté numérique est bien répandue dans le monde et se décline en différents modèles selon la priorité donnée à la régulation ou au contrôle étatique.

L'Union européenne

L'Union européenne (UE) vise à réduire sa dépendance aux fournisseurs technologiques étrangers, à garantir la maîtrise de ses données et à renforcer les infrastructures critiques sur son territoire. Pour y parvenir, l'UE combine des initiatives législatives, des projets d'infrastructures partagées et des investissements publics ciblés dans des solutions infonuagiques et des services numériques « souverains ». Par exemple, depuis plusieurs années, l'UE mise sur le logiciel libre comme levier pour réduire la dépendance envers les grands fournisseurs étrangers.

Parallèlement, des approches complémentaires émergent, telles que l'obligation d'assurer l'interopérabilité des données. Cette mesure permettrait à différents logiciels, peu importe leur origine, de manipuler les mêmes données, contribuant ainsi à éviter les situations de captivité technologique.

⁴ Analyse Forrester : *The State Of Digital Sovereignty In Public Cloud (État de la souveraineté numérique dans le Cloud public)*, 2024

L’Australie

L’Australie a mis en place des mesures ciblées démontrant une volonté d’encadrer certaines dimensions de sa souveraineté numérique. Le gouvernement a évoqué la nécessité que les données sensibles soient hébergées dans des centres de données situés en Australie, et accessibles seulement par du personnel accrédité au pays.

Le Canada

Le gouvernement du Canada a publié en octobre 2025 un cadre⁵ visant à accroître sa résilience, son agilité et sa souveraineté numérique. Associé à la création du Bureau de la transformation numérique, annoncée⁶ au Budget fédéral 2025, ce cadre présente des orientations auxquelles sont en cohérence les orientations proposées dans le présent Énoncé.

Le cadre fédéral mise sur le déploiement sécuritaire et maîtrisé de nouvelles technologies résilientes permettant notamment l’interopérabilité des données. Il met aussi l’accent sur la diversification des fournisseurs en TI et la prévention de la captivité numérique, notamment par l’usage accru de logiciels ouverts et de standards communs. Il prévoit la mise en œuvre d’une identité numérique fédérale, de plateformes partagées et de solutions infonuagiques souveraines. Ce cadre privilégie une approche pragmatique centrée sur la transformation numérique de l’État et sur la réduction des dépendances en TI, tout en renforçant la gouvernance des données et en améliorant les capacités en TI.

Le ministre de la Cybersécurité et du
Numérique,

GILLES BÉLANGER

⁵ [Souveraineté numérique : Un cadre pour améliorer la préparation numérique du gouvernement du Canada - Canada.ca](#)

⁶ Budget fédéral 2025 « Un Canada fort – Budget 2025 », page 245