

ÉNONCÉ DE POLITIQUE DE SOUVERAINETÉ NUMÉRIQUE ET D'APPROVISIONNEMENT EN TECHNOLOGIE DE L'INFORMATION (TI)

MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE



ÉNONCÉ DE POLITIQUE DE SOUVERAINETÉ NUMÉRIQUE ET D'APPROVISIONNEMENT EN TECHNOLOGIE DE L'INFORMATION (TI)

MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE

RÉDACTION

Le Sous-ministériat adjoint aux services à l'organisation et aux clientèles
du ministère de la Cybersécurité et du Numérique

ÉDITION

La Direction des communications du ministère de la Cybersécurité et du Numérique

Le présent document est disponible en version électronique,
à l'adresse [Québec.ca/gouvernement/ministere/cybersecurite-numerique](https://quebec.ca/gouvernement/ministere/cybersecurite-numerique),
dans la section Publications.

Si vous éprouvez des difficultés techniques ou si vous souhaitez obtenir
une version adaptée du document, veuillez communiquer avec la Direction
des communications :

Direction des communications
Ministère de la Cybersécurité et du Numérique
900, place D'Youville, 2^e étage
Québec (Québec) G1R 3P7
Courriel : information@mcn.gouv.qc.ca

Dépôt légal – Février 2026
Bibliothèque et Archives nationales du Québec
ISBN 978-2-555-03008-4 (PDF)

Tous droits réservés pour tous pays. La reproduction, par quelque procédé que ce soit, la traduction
ou la diffusion de ce document, même partielles, sont interdites sans l'autorisation des Publications
du Québec. Cependant, la reproduction de ce document ou son utilisation à des fins personnelles,
d'étude privée ou de recherche scientifique, mais non commerciales, sont permises à condition
d'en mentionner la source.

TABLE DES MATIÈRES

INTRODUCTION	1
1. CONTEXTE	2
2. OBJECTIFS	3
1- Accroître la souveraineté numérique du Québec	3
2- Maximiser les retombées économiques des investissements de l'État en TI	3
3. ORIENTATIONS PROPOSÉES	4
3.1. Objectif : accroître la souveraineté numérique du Québec	4
3.1.1. Favoriser l'hébergement souverain au sein du NGQ et dans les CTI	4
3.1.2. Assurer le contrôle des données par l'intermédiaire, notamment, des centres de données sous juridiction québécoise	4
3.1.3. Renforcer l'utilisation du logiciel libre et soutenir la création de solutions sur mesure	5
3.1.4. Maximiser l'utilisation de la Plateforme de développement moderne (PDM)	5
3.1.5. S'inspirer des meilleures pratiques internationales en matière d'encadrement des TI	6
3.2. Objectif : maximiser les retombées économiques des investissements de l'État en TI	6
3.2.1. Exploiter pleinement les marges de manœuvre disponibles au sein du cadre normatif en gestion contractuelle	6
3.2.2. Bâtir une expertise et une capacité numérique locale fortes	7
3.2.3. Préserver les investissements majeurs en TI au Québec	7
4. ANALYSE COMPARATIVE	8
5. MISE EN ŒUVRE	9

INTRODUCTION

L'Énoncé de politique de souveraineté numérique et d'approvisionnement en technologie de l'information (TI) (Énoncé) pose les bases permettant de faire connaître les objectifs et les orientations que souhaite prendre le gouvernement en ces matières.

Ce socle stratégique servira de point d'ancrage pour élaborer une politique et définir les initiatives prioritaires à mettre en œuvre pour l'organisation de la souveraineté numérique du Québec.

L'Énoncé se veut un acte politique fondateur, permettant de mobiliser l'administration publique et de diriger l'action gouvernementale, en vue du développement, de manière progressive, maîtrisée et en collaboration avec les acteurs gouvernementaux concernés, des modalités concrètes de mise en œuvre des orientations de gouvernance 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 renseignements personnels et la confidentialité des échanges numériques, notamment en ce qui concerne leur hébergement, leur traitement, leur partage et leur protection contre tout accès non autorisé. La souveraineté des données implique que les données sont soumises aux lois du pays dans lequel elles se trouvent.

Proposition

L'Énoncé vise à définir les orientations que le gouvernement du Québec pourrait mettre en place pour renforcer son autonomie numérique tout en maximisant les retombées économiques pour le Québec dans ce domaine.

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.

Le gouvernement du Québec compte de plus en plus sur les technologies du numérique pour améliorer les services qu'il offre à sa population et pour renforcer l'efficacité de l'administration publique. 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.

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.

Plusieurs des projets en ressources informationnelles, actuellement en planification ou en exécution, visent à mettre en place, ou encore à moderniser, des systèmes qui sont utilisés pour traiter des données sensibles, incluant certains renseignements personnels, des citoyens, des citoyennes et des organisations du Québec. Ces systèmes, qui soutiennent des services essentiels à la population, doivent être conformes aux exigences en cybersécurité, en protection des renseignements personnels et en accessibilité.

Pour se positionner comme un modèle exemplaire et un chef de file, l'État doit veiller à ce que sa transformation numérique s'effectue dans un environnement cybersécuritaire, assurant ainsi que les décisions technologiques tiennent compte des risques et des protections nécessaires à chaque niveau d'intervention et que les dispositifs de protection appropriés soient mis en œuvre.

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.

Par ailleurs, le gouvernement s'appuie encore sur des fournisseurs technologiques étrangers pour une partie de ses infrastructures et de ses solutions numériques. Cette réalité met en évidence l'importance stratégique de renforcer l'autonomie numérique du Québec.

En officialisant des orientations structurantes, le Québec pourra affirmer son positionnement en matière de souveraineté numérique et s'assurer que les initiatives numériques gouvernementales s'articulent autour de la maîtrise durable de ses capacités technologiques tout en protégeant ses intérêts pour les générations à venir.

Il est donc capital que le gouvernement du Québec renforce 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.

2- OBJECTIFS

L'Énoncé vise à établir le socle stratégique qui servira de référence pour déterminer les priorités en matière de souveraineté numérique.

Concrètement, il s'articule autour de huit orientations fondées sur deux objectifs centraux.

1- Accroître la souveraineté numérique du Québec

- Favoriser l'hébergement souverain des données au sein du Nuage gouvernemental du Québec (NGQ) et dans les centres de traitement informatique (CTI);
- Assurer le contrôle des données par l'intermédiaire, notamment, des centres de données sous juridiction québécoise;
- Renforcer l'utilisation du logiciel libre et soutenir la création de solutions sur mesure;
- Maximiser l'utilisation de la Plateforme de développement moderne (PDM);
- S'inspirer des meilleures pratiques internationales en matière d'encadrement des TI.

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

- Exploiter pleinement les marges de manœuvre disponibles au sein du cadre normatif en gestion contractuelle;
- Bâtir une expertise et une capacité numérique locale forte;
- Préserver les investissements majeurs en TI au Québec.

3- ORIENTATIONS PROPOSÉES

3.1. Objectif : accroître la souveraineté numérique du Québec

Pour renforcer sa souveraineté numérique, le Québec doit disposer d'un contrôle opérationnel direct sur ses logiciels et applications critiques, ce qui lui assure autonomie et réactivité dans la détection des vulnérabilités et dans la mise en œuvre des correctifs de sécurité nécessaires.

La souveraineté numérique du Québec est un levier essentiel pour accélérer l'autonomie de l'État dans le choix de ses TI et pour renforcer la confidentialité, la sécurité et l'intégrité de ses données numériques, tant sur le plan de l'hébergement que sur le plan de leur transmission par voie de télécommunication.

3.1.1. Favoriser l'hébergement souverain au sein du NGQ et dans les CTI

Accélérer l'expansion et l'évolution du NGQ en diversifiant les services offerts permettrait l'intégration progressive des systèmes et données des organismes publics et favoriserait l'hébergement souverain des données en assurant que les informations sensibles demeurent sous juridiction québécoise, dans des environnements contrôlés localement.

Cette approche réduirait la dépendance à l'égard de fournisseurs externes, améliorerait le contrôle sur les accès, accroîtrait la sécurité et la résilience des infrastructures et garantirait que les données essentielles à la mission de l'État sont régies par les lois du Québec.

Alternative possible au NGQ

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.

3.1.2. Assurer le contrôle des données par l'intermédiaire, notamment, des centres de données sous juridiction québécoise

Le Québec dispose d'une occasion historique pour mettre en place une infrastructure fonduagique souveraine considérant les atouts stratégiques qu'il possède.

Il bénéficie d'une électricité propre, stable, abondante et à coûts compétitifs, d'un cadre réglementaire strict, d'une expertise de plus en plus reconnue en intelligence artificielle (IA) et d'un bassin d'entreprises technologiques en croissance.

La création de centres de données souverains permettrait de renforcer la protection des données de l'État en sol québécois tout en soutenant la recherche et en réduisant la dépendance aux fournisseurs mondiaux d'infonuagique à grande échelle.

Au surplus, la demande mondiale pour ce type d'infrastructure croît de manière exponentielle, portée notamment par la démocratisation de l'IA.

3.1.3. Renforcer l'utilisation du logiciel libre et soutenir la création de solutions sur mesure

Le logiciel libre est l'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 perspectives incontournables pour accélérer ce type de développement personnalisé et permet d'accroître l'agilité technologique tout en stimulant l'expertise locale.

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

3.1.4. Maximiser l'utilisation de la Plateforme de développement moderne (PDM)

La PDM est un environnement intégré que propose de mettre en place le gouvernement du Québec pour standardiser et moderniser le développement des applications et services numériques, notamment les pratiques de cybersécurité associées.

Une telle PDM 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 permettrait de mieux contrôler le cycle de vie des applications, garantirait la sécurité des données et le développement de solutions adaptées aux besoins spécifiques de l'État, favorisant leur mise à l'échelle et réduisant la dépendance aux fournisseurs étrangers.

En assurant au gouvernement du Québec un contrôle opérationnel direct sur les logiciels et applications critiques, l'utilisation de la PDM deviendrait un facteur clé pour bâtir un écosystème numérique souverain.

3.1.5. S'inspirer des meilleures pratiques internationales en matière d'encadrement des 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 (voir la section 4).

À l'instar de pratiques adoptées à l'international, le Québec s'inspirera des expériences d'autres pays pour guider ses propres initiatives. Notamment, lors de l'analyse de mises à jour ou de nouvelles mesures législatives touchant le domaine des TI, il pourrait évaluer la pertinence de recommander des efforts d'harmonisation avec certaines normes et directives internationales en matière de cybersécurité et de numérique, dans la mesure où elles sont compatibles avec les intérêts et les priorités du Québec.

Cette approche permettrait de renforcer la crédibilité et l'efficacité des actions québécoises tout en protégeant nos spécificités et notre autonomie.

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

3.2 Objectif : maximiser les retombées économiques des investissements de l'État en TI

3.2.1. 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 pourrait mieux encadrer ses acquisitions en TI et en services numériques.

Cette approche favoriserait la sélection de solutions conformes aux objectifs de souveraineté numérique, notamment en matière de contrôle des données et d'autonomie technologique.

Elle favoriserait 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 pourrait être envisagée, en fonction des besoins stratégiques ou des risques identifiés, notamment pour consolider la sécurité des données.

3.2.2. Bâtir une expertise et une capacité numérique locale fortes

Développer une expertise et une capacité numérique locale solides est essentiel pour renforcer l'autonomie technologique du Québec et réduire sa dépendance envers des fournisseurs étrangers.

Disposer d'un important bassin d'expertise au Québec permettrait non seulement de sécuriser les infrastructures et services numériques de l'État, mais aussi de renforcer la résilience des services publics, de soutenir la compétitivité économique et de créer des emplois à forte valeur ajoutée.

En développant l'expertise locale, le gouvernement assurerait la maîtrise durable de ses capacités numériques tout en protégeant les intérêts stratégiques de la province. Il deviendrait alors essentiel d'investir dans la formation et le perfectionnement en matière de compétences numériques tout en soutenant l'innovation par l'entremise de partenariats stratégiques avec le secteur numérique québécois, et ce, dans le plein respect des cadres normatifs en vigueur.

3.2.3. 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.

Préserver les investissements majeurs en TI, y compris ceux provenant de l'étranger, contribuerait 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'assurerait d'un écosystème technologique performant sur son territoire : les entreprises renforceraient leurs compétences, formeraient davantage de spécialistes et développeraient des solutions davantage adaptées aux besoins du Québec. À terme, cela pourrait se traduire par une offre plus diversifiée de fournisseurs mieux outillés pour répondre aux différents besoins gouvernementaux.

Protéger les investissements majeurs des entreprises en TI contribuerait également à réduire le risque réputationnel à l'égard de la province quant à la stabilité des investissements en TI, ce qui pourrait influencer la décision d'autres entreprises de s'implanter au Québec.

Conséquemment, les moyens qui pourraient être mis en place dans le cadre d'une politique de souveraineté numérique et d'approvisionnement en TI n'auront pas d'effets contreproductifs ou néfastes au regard des activités économiques d'importance déjà exercées au Québec en matière de TI.

4- 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.

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.

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 cadre¹ visant à accroître sa résilience, son agilité et sa souveraineté numérique. Associé à la création du Bureau de la transformation numérique, annoncée² au Budget fédéral 2025, ce cadre présente des orientations alignées aux 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.

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

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

5- MISE EN ŒUVRE

Si elles sont adoptées, les orientations présentées dans l'Énoncé constitueraient l'assise d'élaboration d'une politique gouvernementale en matière de souveraineté numérique et d'approvisionnement en TI.

Une telle politique gouvernementale permettrait d'établir des orientations claires et cohérentes avec les priorités stratégiques du gouvernement, puis de définir, de planifier et de mettre en œuvre des initiatives concrètes visant à renforcer l'autonomie numérique de l'État.

Les initiatives ciblées seront évaluées individuellement et priorisées au regard, notamment, du degré de sensibilité des données concernées, du coût de réalisation ainsi que du contexte général prévalant.

Des démarches de consultation ciblées auprès des différents acteurs gouvernementaux et une analyse des risques devront être réalisées pour déterminer les initiatives prioritaires à fort impact.

Un plan d'action serait élaboré pour encadrer la mise en œuvre de ces initiatives, en tenant compte des forces et des vulnérabilités du Québec dans l'écosystème du numérique.

En collaboration avec les différents acteurs concernés, des indicateurs de performance devront être prévus pour suivre et évaluer périodiquement l'avancement des initiatives et le degré de mise en application des orientations.

Si une politique gouvernementale était adoptée, après que les priorités auront été ciblées et les travaux amorcés, les organismes publics auraient la responsabilité de veiller à ce que leurs projets et acquisitions en TI soient alignés avec les orientations de souveraineté convenues.

Ils seront également appelés à collaborer entre eux et à mutualiser leurs ressources et leurs expertises pour renforcer l'efficacité et la résilience de l'ensemble de l'écosystème numérique de l'État.

Finalement, la révision périodique d'une telle politique sera nécessaire et prévue, considérant l'évolution rapide du domaine des TI.

