

LES GRANDES TENDANCES EN TRANSFORMATION NUMÉRIQUE DANS LES ADMINISTRATIONS PUBLIQUES

ÉDITION DE JUILLET 2026

MINISTÈRE DE LA CYBERSÉCURITÉ

ET DU NUMÉRIQUE

RÉDACTION

Sous-ministériat adjoint aux partenariats et à l'intelligence artificielle du ministère de la Cybersécurité et du Numérique

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
425, rue Jacques-Parizeau
Québec (Québec) G1R 5E4
Téléphone : 418 644-1030
Courriel : information@mcn.gouv.qc.ca

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, est permise à condition d'en mentionner la source.

TABLE DES MATIÈRES

Introduction	3
Le passage de l'IA expérimentale à l'IA opérationnelle.....	3
L'émergence de l'État agentique.....	4
La souveraineté numérique devient une priorité stratégique.....	4
La cybersécurité entre dans une nouvelle phase	5
La donnée devient l'actif stratégique principal	6
Perspectives pour le second semestre 2026	6
Conclusion	6
Références.....	7

INTRODUCTION

Jusqu'à maintenant, l'année 2026 est marquée par un point de bascule dans la transformation numérique des administrations publiques. Après une période dominée par l'expérimentation, notamment en intelligence artificielle (IA), les gouvernements entrent dans une phase de mise à l'échelle où les technologies doivent produire des gains mesurables en performance, en qualité des services et en résilience organisationnelle. Cette transition s'effectue dans un contexte de contraintes budgétaires, de hausse des attentes citoyennes, d'intensification des cybermenaces et de tensions géopolitiques qui redéfinissent les choix technologiques publics.

Les analyses récentes de l'Organisation de coopération et de développement économique (OCDE) indiquent que les technologies numériques et les données ne constituent plus de simples outils d'amélioration administrative. Elles forment désormais une infrastructure essentielle à la capacité d'action de l'État. Le défi central n'est donc plus seulement de construire des fondations numériques, mais de les convertir en retombées concrètes pour les citoyens, les entreprises et les organisations publiques.

Depuis janvier 2026, cinq tendances structurantes se dégagent : l'industrialisation de l'IA, l'émergence de l'État agentique, la souveraineté numérique, l'évolution de la cybersécurité et la valorisation stratégique des données.

LE PASSAGE DE L'IA EXPÉRIMENTALE À L'IA OPÉRATIONNELLE

La tendance la plus marquante de 2026 est sans contredit le passage de l'expérimentation à la démocratisation de l'intelligence artificielle.

Entre 2023 et 2025, plusieurs administrations ont testé des assistants conversationnels, des outils de rédaction automatisée et des solutions de synthèse documentaire. En 2026, l'attention se porte désormais sur l'intégration de ces solutions dans les processus courants, avec des attentes explicites en matière de productivité, de qualité du service et de réduction des délais. Cette évolution impose de passer d'une logique de projets pilotes à une logique de portefeuille, de priorisation et de gestion des bénéfices.

L'OCDE observe que l'IA est désormais utilisée dans au moins un domaine gouvernemental dans la quasi-totalité des pays membres. Toutefois, peu d'administrations évaluent systématiquement les effets financiers et non financiers de ces usages. Cette lacune place la mesure des résultats, la reddition de comptes et la gestion des risques au centre de la prochaine étape de maturité.

Au Québec, les travaux qui démarrent entourant l'actualisation de la stratégie gouvernementale en intelligence artificielle s'inscrivent dans cette dynamique. Les discussions portent sur l'IA générative, l'IA agentique, l'IA physique et leur contribution possible à la productivité, à la compétitivité, à la souveraineté numérique et à l'amélioration des services publics.

Les fonctions les plus susceptibles d'être transformées sont le service à la clientèle, la gestion documentaire, les fonctions administratives, les ressources humaines, l'analyse décisionnelle, la cybersécurité et le développement logiciel. La valeur ne résidera toutefois pas seulement dans les outils, mais dans la capacité des organisations à revoir leurs processus, leurs contrôles et leurs compétences.

L'ÉMERGENCE DE L'ÉTAT AGENTIQUE

Une deuxième tendance majeure en 2026 est l'apparition des systèmes d'IA agentique, c'est-à-dire des agents autonomes capables de réaliser des tâches complexes en exécutant plusieurs actions de manière coordonnée.

Contrairement aux assistants conversationnels, qui répondent principalement à des requêtes ponctuelles, les agents peuvent planifier une séquence d'actions, consulter plusieurs systèmes, analyser des données et déclencher certaines opérations dans un cadre défini. Deloitte présente cette évolution comme l'un des leviers majeurs de personnalisation et de simplification des services publics.

Cette évolution annonce un « État agentique » dans lequel certaines fonctions répétitives ou transactionnelles, que ce soit par exemple le traitement des demandes, la validation documentaire, la gestion de dossiers, la surveillance réglementaire ou le soutien aux opérations, pourraient être partiellement automatisées, tout en demeurant encadrées par des responsabilités humaines clairement établies.

Le potentiel est important, mais les risques le sont tout autant, en matière notamment de l'attribution de la responsabilité, de la traçabilité des décisions, de la supervision humaine ou encore de la protection des renseignements personnels. L'enjeu pour toute administration publique n'est donc pas seulement d'adopter des agents, mais de définir les conditions dans lesquelles ils peuvent agir de façon fiable, proportionnée et vérifiable.

LA SOUVERAINETÉ NUMÉRIQUE DEVIENT UNE PRIORITÉ STRATÉGIQUE

Depuis le début de 2026, la souveraineté numérique est passée d'un enjeu technique à un enjeu stratégique de premier ordre.

Les tensions géopolitiques, les débats sur l'hébergement des données et la concentration du marché technologique amènent les gouvernements à réévaluer leurs dépendances envers les grandes plateformes étrangères. La souveraineté numérique touche désormais l'infonuagique, l'intelligence artificielle, l'identité numérique, la cybersécurité, les données gouvernementales et les mécanismes d'approvisionnement.

Les analyses prospectives de Forrester anticipent une montée du « nationalisme technologique », soit une préférence accrue pour des solutions nationales, régionales ou juridiquement maîtrisées dans les usages critiques. Pour les administrations publiques, cette tendance ne signifie pas l'autarcie technologique, mais une gestion plus stratégique des dépendances, des risques contractuels et de la localisation des actifs numériques.

Cette orientation influence directement les choix d'architecture, les exigences de sécurité, les modèles contractuels, les politiques d'approvisionnement ou encore les critères d'encadrement de l'IA. Elle impose également de mieux distinguer les usages courants, qui peuvent s'appuyer sur des solutions commerciales, des usages critiques, qui exigent des garanties renforcées.

LA CYBERSÉCURITÉ ENTRE DANS UNE NOUVELLE PHASE

La cybersécurité demeure une priorité absolue en 2026, car les risques évoluent plus rapidement que jamais. Les attaques traditionnelles sont désormais renforcées par l'IA, qui facilite l'automatisation des intrusions, la production de contenus synthétiques, la création de faux documents et la génération de voix ou de vidéos falsifiées.

Dans ce contexte, l'identité numérique devient un point névralgique. Les hypertrucages, l'hameçonnage sophistiqué et la compromission des accès accentuent la nécessité de renforcer l'authentification, la gestion des identités et les mécanismes de détection des comportements anormaux.

Parallèlement, plusieurs organisations adoptent des approches reposant sur le modèle à vérification systématique (*zero trust*), l'automatisation de la détection, l'analyse comportementale ou l'IA défensive.

KPMG indique que 64 % des organisations gouvernementales prévoient augmenter leurs investissements en cybersécurité au cours de la prochaine année, ce qui confirme le passage d'une logique de protection périphérique à une logique de résilience continue.

Un autre sujet gagne rapidement en importance, soit la préparation à la cryptographie postquantique. Plusieurs administrations commencent à planifier la migration de leurs infrastructures afin de se prémunir contre les futures capacités de calcul quantique.

LA DONNÉE DEVIENT L'ACTIF STRATÉGIQUE PRINCIPAL

La donnée devient l'actif stratégique principal de l'État numérique. En 2026, cette réalité est accentuée par le déploiement de l'IA à grande échelle, laquelle dépend directement de la qualité, de la disponibilité, de la documentation et de l'interopérabilité des données.

Même lorsque les stratégies de données sont relativement matures, plusieurs administrations peinent encore à assurer l'interopérabilité entre systèmes, à partager l'information de manière sécuritaire et à maintenir des référentiels fiables. Ces limites freinent la personnalisation des services, la prise de décision fondée sur les données et l'automatisation responsable.

Les administrations qui maîtriseront la gouvernance des données seront les mieux placées pour tirer parti de l'IA, réduire les silos, améliorer la qualité des services et renforcer la capacité d'analyse stratégique de l'État.

PERSPECTIVES POUR LE SECOND SEMESTRE 2026

Pour le reste de l'année 2026, les administrations publiques devraient accélérer le passage des projets exploratoires vers des usages intégrés et mesurables. Les projets d'IA devront démontrer leur valeur en matière de productivité, de qualité du service, de rapidité de traitement et de réduction des irritants administratifs.

Les gouvernements devraient également renforcer leurs cadres de gouvernance de l'IA afin de répondre aux attentes de transparence, de responsabilité et de confiance publique. Les mécanismes d'évaluation, de traçabilité, de gestion des risques et de reddition de comptes deviendront déterminants pour soutenir le passage à l'échelle.

La souveraineté numérique devrait aussi prendre davantage de poids dans les décisions d'investissement, d'approvisionnement et d'architecture technologique. L'hébergement des données, l'origine des modèles, la réversibilité contractuelle et la dépendance aux fournisseurs deviendront des critères de décision plus explicites.

Enfin, les initiatives liées à l'identité numérique, aux services proactifs et aux cadres de confiance numérique devraient s'accélérer, en particulier dans les juridictions qui ont déjà investi dans des données mieux structurées, une gouvernance robuste et une architecture numérique cohérente.

CONCLUSION

La première moitié de 2026 confirme que la transformation numérique gouvernementale entre dans une phase plus exigeante. Les administrations publiques ne cherchent plus

seulement à expérimenter l'IA, l'infonuagique ou les données. Elles se doivent d'intégrer ces leviers dans leurs opérations, en mesurer les effets et en maîtriser les risques.

L'intelligence artificielle, surtout dans ses formes générative et agentique, constitue le principal moteur de cette nouvelle étape. Son déploiement ne pourra toutefois produire de valeur durable que s'il repose sur des données fiables et intégrées aux processus, une cybersécurité renforcée, des compétences adaptées et une gouvernance publique robuste.

Pour l'administration publique québécoise comme pour ses homologues internationales, l'enjeu des prochains mois sera donc moins technologique qu'organisationnel, c'est-à-dire qu'il faudra transformer les investissements numériques des dernières années en gains durables de performance, de confiance citoyenne et de valeur publique.

RÉFÉRENCES

Principales sources

- OCDE, [Perspectives de l'administration numérique 2026](#)
- OCDE, [AI in Government: Publications](#)
- Deloitte, [GovTech Trends 2026](#)
- KPMG, [Global tech report 2026 : Government and public sector](#)
- Capgemini, [Public Administration Trends 2026 in a Digital World](#)
- NTT DATA, [From readiness to results: Five public sector trends defining 2026](#)

