

L'IA ET LA LOI 25 : PRÉVENIR LES RISQUES NUMÉRIQUES



Pourquoi cette fiche ?

De plus en plus de municipalités québécoises expérimentent et intègrent des systèmes d'intelligence artificielle (IA) dans leurs services. Or, cela transforme en profondeur la gestion des données et pose des défis importants de cybersécurité, de transparence et de protection de la vie privée.

Avec l'entrée en vigueur progressive de la Loi 25, les municipalités doivent adapter leurs pratiques, surtout lorsque des systèmes automatisés traitent des renseignements personnels. L'IA accentue l'importance de comprendre ces risques, de sécuriser les données, de documenter les processus et de mobiliser les bons acteurs.

Cette fiche propose des conseils pratiques et des outils adaptés au contexte municipal pour encadrer vos projets d'IA, respecter la Loi 25 et renforcer votre cybersécurité.

Bonnes pratiques en cybersécurité appliquée à l'IA

L'anonymisation en IA est difficile à garantir, car le croisement de données peut mener à une réidentification. Il est essentiel de tester ce risque, de réduire la granularité des données et de ne pas considérer l'anonymisation comme suffisante pour se conformer à la loi 25.

QUELQUES PRATIQUES CLÉS :

- Contrôle des accès, journalisation, et chiffrement des flux de données;
- Documentation technique complète (origine des données, versions, fournisseurs, risques identifiés);
- Validation et supervision humaine obligatoire pour les processus critiques (ex : attribution d'aide, sanction);
- Plan de réponse aux incidents incluant les spécificités des systèmes IA;
- Information claire aux citoyens sur l'usage de l'IA (rôle, type de traitement, niveau de contribution, implications).

AVANT L'IA, LA BASE

Plusieurs municipalités n'ont pas encore atteint le strict minimum en cybersécurité selon les standards établis. L'IA ajoute des exigences et complexifie la sécurité. Avant de lancer un projet d'IA, il est crucial de :

- Effectuer un audit de cybersécurité basé sur un référentiel reconnu;
- Mettre en place les mesures minimales (gestion des identités, segmentation réseau, plan de réponse aux incidents, sauvegardes testées);
- Former le personnel aux risques numériques

L'acceptabilité sociale est aussi un facteur critique :

- impliquer les citoyens en amont, consulter sur les usages sensibles et documenter les enjeux éthiques aide à prévenir la méfiance et à ajuster les projets à la réalité locale.

POINTS IMPORTANTS À RETENIR



La Loi 25 a profondément réformé la façon dont les renseignements personnels doivent être protégés au Québec, et son application à l'IA municipale est aujourd'hui incontournable. Tout projet intégrant des chatbots, de l'analyse automatisée ou du profilage se doit de respecter des obligations strictes.

Sans ce cadre, la municipalité s'expose non seulement à des **sanctions financières** importantes et une **érosion de la confiance citoyenne**, ce qui peut directement dégrader de la qualité du service public et l'affaiblissement de la sécurité des données.



La loi 25 : obligations clés

La Loi 25 impose plusieurs obligations aux municipalités en matière de traitement automatisé :

- Tenue d'un registre des traitements automatisés;
- Réalisation et mise à jour régulière d'une évaluation des facteurs relatifs à la vie privée (EFVP) pour chaque système d'IA;
- Consentement explicite et information claire des citoyens;
- Limitation de l'accès et conservation encadrée des renseignements personnels.

BON À SAVOIR

- Les données anonymisées ne sont pas soumises à la Loi 25.

DÉLAI DE CONFORMITÉ

- Depuis le 22 septembre 2024, toutes les dispositions s'appliquent pleinement et la conformité est exigée immédiatement, sans période de grâce.

Un déploiement sécuritaire en 3 étapes

PHASE 1 - PRÉPARATION

- Cartographie des données;
- Choix technologiques conformes aux exigences de conformité;
- Implication des RH, TI et services juridiques.

PHASE 2 : DÉPLOIEMENT

- Tests préalables (qualité, biais, robustesse);
- Vérification de la conformité des prestataires (confidentialité par défaut, notification d'incident, localisation des serveurs, auditabilité);
- Clauses contractuelles de responsabilité;
- Mise en place de garde-fous techniques et humains.

PHASE 3 : SUIVI

- Suivi des performances;
- Canal de signalement d'anomalies;
- Formations continues et mise à jour de la documentation;
- Plan de sortie du système IA (suppression sécurisée des données, désactivation des accès, archivage réglementaire).

Éléments opérationnels clés par acteur



ÉLUS MUNICIPAUX

- Valident les orientations stratégiques d'intégration de l'IA et leur adéquation avec les attentes citoyennes;
- Assurent la conformité éthique des projets d'IA;
- Demandent régulièrement des comptes rendus sur les impacts et risques liés à l'IA;
- Promeuvent une gouvernance transparente et participative impliquant les citoyens.



DIRECTION GÉNÉRALE

- Pilote et coordonne l'intégration de l'IA au sein des services;
- Met en place un cadre clair de gouvernance interne (politiques, procédures, mécanismes de contrôle);
- Évalue régulièrement l'impact opérationnel, humain et financier des solutions déployées;
- Mobilise les ressources nécessaires pour accompagner la transition numérique vers l'IA.



DIRECTION DES RH

- Forme les employés à la cybersécurité et à la responsabilité numérique;
- Appuie les changements organisationnels induits par l'IA.



SERVICE TI

- Gère la sélection, l'intégration, la sécurité et l'évolution des systèmes d'IA;
- Met en place des protections robustes (chiffrement, gestion des accès, etc.);
- Déploie des audits réguliers pour détecter des biais, erreurs ou vulnérabilités;
- Valide les fournisseurs et intègre les systèmes selon les exigences de sécurité;
- Gère les mises à jour, la journalisation et les incidents;
- Assure la documentation détaillée des systèmes (origine des données, paramètres techniques, traçabilité).



EMPLOYÉS MUNICIPAUX

- Appliquent les protocoles de sécurité;
- Signalent toute anomalie ou utilisation douteuse;
- Participent aux formations et adoptent les réflexes de prudence.

BOÎTE À OUTILS



Dans cette boîte à outils, vous trouverez des ressources pratiques pour passer à l'action : gabarits d'évaluation EFVP, exemples de politiques internes, guides de cybersécurité, clauses contractuelles types à intégrer avec vos fournisseurs d'IA, ainsi que des liens vers plusieurs guides.



Lien cliquable