Prévenir un nouveau fiasco : pistes de solution pour les projets gouvernementaux

(Document de travail préparé pour la Commission Gallant – 15 septembre 2025)

Préambule

Ce document a été rédigé comme outil de travail pour soutenir la réflexion de la Commission Gallant. Son objectif n'est pas de commenter uniquement le dossier SAAQclic, mais de proposer des pistes de solution afin d'éviter qu'un scénario similaire ne se reproduise dans le cadre d'autres projets gouvernementaux, qu'ils soient technologiques ou non.

Il est important de préciser que l'analyse qui suit représente mon point de vue extérieur à la Commission, en date du 15 septembre 2025. Il reviendra au Commissaire Gallant et à son équipe de déterminer de façon officielle les causes profondes des échecs observés et les recommandations formelles.

Enfin, je tiens à souligner que les problématiques décrites ici ne sont pas propres à la SAAQ. J'ai pu observer et relever des enjeux similaires au ministère de la Cybersécurité et du Numérique (MCN), à la Sûreté du Québec (SQ) et au ministère des Relations internationales et de la Francophonie (MRIF). Ces constats m'amènent à conclure qu'il s'agit de problèmes systémiques, liés à la gouvernance, à la culture organisationnelle et à l'absence d'imputabilité réelle dans l'appareil gouvernemental.

Constat – Trois problèmes majeurs

1- Opacité et dilution des responsabilités

Les défaillances majeures sont rarement attribuées à une personne ou une équipe précise. Les responsabilités se diluent à travers de multiples niveaux hiérarchiques, ce qui crée une impression que « quelqu'un d'autre » est responsable. C'est le même mécanisme psychologique qui permet à un

enfant de se noyer dans une piscine entourée d'adultes : chacun croit que l'autre surveille.

2- Culture hiérarchique qui filtre et masque l'information

La structure organisationnelle actuelle agit comme une série de coupe-feux qui protègent les gestionnaires supérieurs plutôt que l'intérêt public. L'information est filtrée en chemin, perdant en transparence et en pertinence, ce qui retarde les décisions correctives.

3- Absence d'expertise indépendante rattachée directement aux décideurs

Les hauts dirigeants ne disposent pas toujours d'un accès direct à une expertise neutre et spécialisée en sécurité et en technologies. Cela favorise une dépendance aux rapports internes biaisés, ou encore à des fournisseurs privés ayant des intérêts propres.

Trois ensembles de solutions

1. Transparence et imputabilité

(Répond au problème : Opacité et dilution des responsabilités)

1.1. Indicateurs de suivi indépendants

Les finances et les performances doivent être suivies par une instance externe (ex. Vérificateur général, Contrôleur des finances).

1.2. Tableau de bord public

Un suivi trimestriel simplifié et accessible à la population renforcerait la transparence et la confiance.

1.3. Post-mortem systématique et public

Chaque projet doit se conclure par un bilan détaillé, publié intégralement, pour tirer des leçons et ajuster les pratiques.

1.4. Imputabilité réelle

Les gestionnaires responsables de graves échecs ne doivent pas être recyclés ailleurs dans l'appareil gouvernemental ou réintégrés comme sous-traitants avant plusieurs années.

1.5. Infractions pénales spécifiques

Utilisation de canaux parallèles interdite (Gmail, Signal, WhatsApp, etc.).

Interdiction de destruction de preuves (courriels, documents, fichiers).

Rétention d'information critique passible de sanctions.

Pressions sur un lanceur d'alerte pénalisées (menaces, blocage de carrière, atteinte à la réputation).

Notes personnelles interdites : tout document relatif à un dossier doit être intégré au dossier officiel.

Interdiction de destruction de notes lors d'un licenciement, d'une démission ou de la perte d'une élection.

2. Hiérarchie simplifiée et circulation de l'information

(Répond au problème : Culture hiérarchique qui filtre et masque l'information)

2.1. Réduction des couches hiérarchiques

Moins de niveaux décisionnels afin de limiter les filtres et d'accélérer la remontée de l'information.

2.2. Canaux directs d'information

Permettre aux employés de première ligne de remonter leurs constats directement vers les décideurs stratégiques ou les experts indépendants.

2.3. Phasage obligatoire des projets

Débloquer les fonds par étapes (« go / no go »), conditionnés à des validations externes, afin de limiter les dérives précoces.

3. Expertise indépendante et gouvernance adaptée

(Répond au problème : Absence d'expertise indépendante)

3.1. Postes-conseils spécialisés

Création de rôles permanents d'experts en sécurité et en technologie rattachés directement aux hauts dirigeants, avec accès direct au terrain. Des projets pilotes menés au MCN et à la SQ ont démontré que l'intégration d'experts indépendants fonctionnait, mais ces approches ont été abandonnées car elles dérangeaient les gestionnaires qui contrôlaient l'information.

3.2. Séparation claire des rôles

La transformation numérique, les TI et la performance organisationnelle doivent relever d'un ministère distinct. La sécurité doit être confiée à une entité autonome et spécialisée.

3.3. Ministère de la sécurité intérieure

Mettre en place un ministère regroupant toutes les dimensions de la sécurité (physique, informationnelle, cybersécurité, filtrage de sécurité, résilience). Ce ministère devrait relever directement du Premier ministre et/ou se situer hiérarchiquement au-dessus des autres.

3.4. Éviter la réduction de la sécurité à la cybersécurité

La sécurité ne doit pas être limitée à la sphère technologique. Elle englobe aussi la protection des personnes, des infrastructures et des processus.

Résumé

L'échec de SAAQclic révèle trois failles systémiques

1. Opacité et dilution des responsabilités.
2. Culture hiérarchique qui filtre et masque l'information.
3. Absence d'expertise indépendante rattachée directement aux décideurs.

Les solutions passent par une triple réforme

1. Transparence et imputabilité pour responsabiliser les gestionnaires et garantir une reddition de comptes réelle.
2. Hiérarchie simplifiée et circulation fluide de l'information pour mettre fin aux filtres et protéger l'intérêt public.
3. Expertise indépendante et gouvernance adaptée afin que les décisions stratégiques reposent sur la compétence, la neutralité et une vision globale de la sécurité.

Conclusion

La modernisation de l'État ne peut réussir sans une transformation profonde de la culture de gestion. Les erreurs observées dans le dossier SAAQclic ne sont pas isolées : elles découlent de mécanismes structurels qui se répéteront tant qu'ils ne seront pas corrigés.

Il faut briser les mécanismes de protection internes qui favorisent l'opacité et replacer la compétence, la transparence et la responsabilité individuelle au centre de l'action publique.