Ministère de la Cybersécurité et du Numérique
Québec

Mesures applicables lors de l'utilisation de l'intelligence artificielle générative

Statut	En vigueur
Diffusion	Restreinte
No de référence	IA-RI-2025-003-OP
Organismes visés	Organismes publics
Indication formulée par	Dirigeant principal de l'information
Référence légale	LGGRI (chapitre G-1.03), art. 7
Date de formulation	2025-12-05
Date d'entrée en vigueur	2025-12-05
Dernière mise à jour	S. O.
Expiration	Indéterminée

SECTION I
DISPOSITIONS INTRODUCTIVES

1. La présente indication d'application prévoit des mesures applicables lors de l'utilisation de l'intelligence artificielle générative[1] (ci-après « IAG ») par les organismes publics.

Elle complète les orientations en matière de ressources informationnelles déterminées par l'arrêté numéro 2025-02 du ministre de la Cybersécurité et du Numérique en date du 3 décembre 2025 concernant une modification à l'arrêté numéro 2024-02 en date du 27 juin 2024 concernant l'Énoncé de principes pour une utilisation responsable de l'intelligence artificielle pour les organismes publics.

2. La présente indication d'application s'applique aux organismes publics visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03).

SECTION II
GOUVERNANCE ORGANISATIONNELLE POUR LES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

§ 1.- Instauration d'une structure de gouvernance adaptée au contexte de l'organisation

3. Un organisme public doit mettre en place une structure de gouvernance adaptée aux besoins de son organisation, assurant ainsi une utilisation responsable des systèmes d'IAG. Il doit s'assurer que cette structure de gouvernance soit arrimée à la gouvernance des données numériques gouvernementales (ci-après « DNG »).

À ce titre, il doit :

1° définir les rôles et les responsabilités en termes de gouvernance des systèmes d'IAG, tel que la ou les personnes ayant l'autorité d'autoriser l'utilisation d'un système d'IAG;

2° constituer les comités ou les groupes de travail appropriés ou élargir les mandats des comités ou groupes de travail existants à des fins de coordination et de concertation en matière de systèmes d'IAG;

3° prévoir un encadrement adapté au contexte de l'organisation favorisant le développement et le déploiement efficaces et responsables d'un système d'IAG;

[1] Ensemble des techniques d'intelligence artificielle utilisées pour produire du contenu au moyen d'algorithmes et de mégadonnées, généralement sous forme de fichier texte, son, vidéo ou image ». *Office québécois de la langue française.*

Ministère de la Cybersécurité et du Numérique
Québec

4° élaborer et tenir à jour un processus d'évaluation clair et documenté pour tout système d'IAG en fonction des cas d'usage[2] de ce système. Le processus s'applique tout au long du cycle de vie du système[3];

5° élaborer et tenir à jour un processus décisionnel permettant aux autorités de l'organisme public de faire des choix éclairés au regard de tous les risques liés aux systèmes d'IAG.

En fonction des cas d'usage identifiés et priorisés, un organisme public est responsable de définir, d'élaborer et d'appliquer les exigences ainsi que les contrôles nécessaires à l'utilisation du système d'IAG qu'il entend concevoir, acquérir, expérimenter ou mettre en œuvre.

§ 2.- Gestion des risques liés à l'utilisation des systèmes d'intelligence artificielle générative

4. Toute utilisation d'un système d'IAG doit être basée sur une démarche de gestion des risques.

Cette démarche doit être exhaustive; elle doit notamment comprendre les étapes qui suivent :

1° identifier tous les risques organisationnels encourus par l'utilisation d'un système d'IAG. Ces risques peuvent, sans s'y limiter, être observés dans les matières suivantes : éthique, sécurité de l'information, gouvernance de données, juridique;

2° analyser les risques (documenter leurs principales causes et conséquences);

3° évaluer les risques et, en fonction notamment des résultats, prioriser leur traitement;

4° déterminer des mesures de mitigation, les responsables de leur mise en œuvre ainsi que leurs échéances;

5° approuver les résultats;

6° effectuer le suivi et la revue des risques en fonction du processus organisationnel défini.

Dès la phase de conception d'un projet d'acquisition, de développement ou de refonte d'un système d'IAG, et lors de la définition des cas d'usage, l'organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée (ci-après « ÉFVP »). Cette ÉFVP doit être actualisée tout au long des phases d'expérimentation, de développement et de déploiement du projet qui concerne un système d'IAG. Le cas échéant, l'autorité désignée au sein de l'organisme doit accepter le niveau de risque résiduel d'atteinte à la vie privée pour poursuivre les activités. Cette exigence vaut pour tous les systèmes d'IAG incluant ceux qui, à première vue, ne semblent pas impliquer de renseignements personnels. Dans le cas de ces derniers, l'organisme public doit procéder à l'ÉFVP laquelle pourra confirmer l'absence de renseignements personnels.

La démarche de gestion des risques visée au premier alinéa, incluant l'ÉFVP, doit être révisée périodiquement en fonction de l'évolution du système d'IAG et de son contexte d'utilisation.

[2] Cas d'usage : description des exigences comportementales d'un système et de son interaction avec un utilisateur [ISO, 2018]. Un cas d'usage décrit l'objectif des utilisateurs ainsi que les exigences, y compris la séquence d'interactions entre les utilisateurs et le système.
[3] Phases d'un cycle de vie de tels systèmes, notamment la phase de planification et de conception, la phase de collecte et de traitement des données, la phase de construction du modèle concerné ou l'adaptation d'un modèle existant pour des tâches spécifiques, la phase de test, d'évaluation, de vérification et de validation, la phase de mise à disposition pour son utilisation, la phase d'exploitation et de suivi et la phase de mise hors service.

Ministère de la Cybersécurité et du Numérique
Québec

5. L'organisme public doit privilégier un modèle d'IAG ouvert[4] lorsque le contexte nécessite une traçabilité complète et une reproductibilité des résultats notamment s'il touche des services destinés aux citoyens ou aux entreprises quand les cas d'usage impliquent des données confidentielles.

§ 3.- Mise en place de mécanismes de contrôle des systèmes d'intelligence artificielle générative

6. Un organisme public doit établir un processus d'amélioration continue pour chaque système d'IAG utilisé, le documenter et l'appliquer. Ce processus vise à s'assurer que le système d'IAG demeure efficace et conforme à une utilisation responsable. Celui-ci doit inclure des vérifications périodiques de la performance ainsi que des revues régulières des pratiques permettant de détecter rapidement les comportements inadmissibles ou les dérives dans l'utilisation d'un système d'IAG. Sans s'y limiter, les comportements inadmissibles peuvent concerner l'utilisation de renseignements confidentiels ou le non-respect des exigences de sécurité de l'information.

Un organisme public doit, préalablement à son déploiement et jusqu'à sa mise hors service, mettre en place des mesures pour vérifier la fiabilité et la robustesse des systèmes d'IAG. Il doit notamment procéder à des essais qui incluent la validation du comportement du système d'IAG lorsque celui-ci doit répondre à des demandes qui pourraient générer des réponses erronées (par exemple : hallucinations, biais) ou lorsqu'il reçoit des demandes auxquelles il ne devrait pas répondre.

SECTION III
GESTION ET PROTECTION DES DONNÉES NUMÉRIQUES GOUVERNEMENTALES EN VUE DE L'UTILISATION DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

§ 1.- Gestion adéquate des données numériques gouvernementales utilisées dans les cas d'usage des systèmes d'intelligence artificielle générative tout au long de leur cycle de vie

7. Un organisme public doit, avant le déploiement de tout système d'IAG, connaître les DNG qui seront utilisées par celui-ci.

Une gestion rigoureuse du cycle de vie des DNG est essentielle afin d'assurer leur qualité, leur sécurité et leur conformité tout au long de leur cycle de vie. Ainsi, la création, la collecte, la conservation, l'utilisation, la transmission, la communication, l'archivage et la destruction des données doivent se faire dans le respect des lois et des textes d'application ainsi que des bonnes pratiques en matière de gestion des données, de gestion documentaire et de protection des renseignements confidentiels.

§ 2.- Classification et sécurisation des données numériques gouvernementales avant leur utilisation dans les cas d'usage des systèmes d'intelligence artificielle générative

8. Un organisme public doit, avant de déployer tout système d'IAG, avoir attribué un profil de mesures de sécurité ou, selon le cas, avoir marqué les DNG utilisées pour chaque cas d'usage.

Il doit s'assurer que les données sont classifiées de manière à limiter l'accès du système d'IAG qu'aux données autorisées et nécessaires pour chaque cas d'usage. Cette étape de classification est essentielle. Elle permet de déterminer le niveau de sécurité nécessaire pour ces données. Elle aide également à appliquer la gestion des accès, comme prévu à l'article 10, pour prévenir toute utilisation non autorisée des renseignements confidentiels.

9. Un organisme public doit, avant de déployer tout système d'IAG, avoir classifié les DNG nécessaires aux cas d'usage priorisés, conformément au modèle de classification de sécurité des données numériques gouvernementales et après avoir appliqué les contrôles prévus au seuil minimal de sécurité.

[4] Un modèle d'IAG ouvert est un modèle dont au moins certains des composants (code, paramètres finaux, documentation, etc.) sont rendus publiquement accessibles et ce, dans un cadre de licences et d'informations qui permettent son usage, son étude, sa modification ou sa redistribution. Le degré d'ouverture peut varier.

Ministère de la Cybersécurité et du Numérique
Québec

Lorsque les DNG utilisées comprennent des renseignements confidentiels, un tel organisme doit également favoriser, lorsque possible, des fournisseurs québécois ou d'ailleurs au Canada offrant des solutions hébergées au Québec ou au Canada.

§ 3.- Gestion des accès aux données numériques gouvernementales pour assurer un contrôle strict des droits d'accès aux données et aux systèmes d'intelligence artificielle générative

10. Un organisme public doit appliquer une gestion stricte des accès aux DNG, laquelle :

1° est essentielle pour assurer une utilisation responsable des systèmes d'IAG;

2° permet d'assurer l'intégrité, la disponibilité et, la confidentialité des données;

3° vise à prévenir toute destruction, modification involontaire ou accès non autorisé.

SECTION IV
INTÉGRATION ET UTILISATION RESPONSABLE DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE PAR LE PERSONNEL DES ORGANISMES PUBLICS

§ 1.- Compétences du personnel et sensibilisation aux risques associés aux systèmes d'intelligence artificielle générative

11. Un organisme public doit élaborer et mettre en œuvre un programme de formation et de sensibilisation aux risques liés à l'utilisation de systèmes d'IAG, lequel prévoit une mise à jour des connaissances lorsque nécessaire.

Ce programme de formation doit être offert au personnel de l'organisme public avant le déploiement du système d'IAG qu'il aura à utiliser. Le programme doit permettre de faire connaître les risques associés à cette technologie et s'assurer d'une utilisation responsable et sécuritaire.

Le programme visé au premier alinéa doit inclure minimalement les formations que peut proposer en ces matières le ministère de la Cybersécurité et du Numérique.

12. Un organisme public doit assurer une gestion du changement adaptée à l'impact organisationnel de l'introduction d'un système d'IAG et permettre l'introduction de cette technologie de manière optimale.

§ 2.- Compétences du personnel pour traiter et appliquer de manière responsable les cas d'usage des systèmes d'intelligence artificielle générative autorisés par un organisme public

13. Un organisme public doit veiller à ce que les membres concernés de son personnel disposent des compétences pour utiliser les systèmes d'IAG de manière responsable, comme prévu à l'Énoncé de principes pour une utilisation responsable de l'intelligence artificielle.

§ 3.- Prioriser les cas d'usage et assurer leur mise en œuvre

14. Un organisme public doit identifier et prioriser les cas d'usage des systèmes d'IAG en s'assurant d'un retour sur investissement, de l'obtention de bénéfices et d'une gestion des risques adéquate.

15. Un organisme public doit s'assurer, pour les cas d'usage qui sont autorisés, que les systèmes d'IAG qu'il utilise et qui ont un impact sur des décisions, des prédictions ou des actions concernant les citoyens ou les entreprises, intègrent des mécanismes qui assurent des explications claires et sans ambiguïté. Pour ces cas, l'utilisation de modèles d'IAG ouverts, lorsque cela est possible, doit être privilégiée.

Ministère de la Cybersécurité et du Numérique
Québec

16. Un organisme public doit, afin d'assurer l'efficience et la qualité des résultats, privilégier l'utilisation d'un modèle d'IAG spécialisé (ou vertical) lorsqu'il est disponible et économiquement viable.

17. Un organisme public doit viser une utilisation efficace et sécurisée des systèmes d'IAG en prévoyant :

1° des lignes directrices internes qui doivent minimalement préciser au bénéfice des membres du personnel les éléments suivants :

- Les cas d'usage qui sont autorisés à recourir à un système d'IAG;
- Les cas d'usage où il est interdit de recourir à un système d'IAG ou qui sont soumis à des restrictions;

2° une supervision humaine assurée de manière proportionnée, par du personnel qualifié, à l'égard de l'impact potentiel des décisions et en tenant compte du degré d'autonomie dont dispose le système d'IAG utilisé;

3° un suivi continu, en effectuant une analyse des impacts, avant et après le déploiement de ces systèmes.

SECTION V
UTILISATION ENCADRÉE DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE PUBLICS

§ 1.- Utilisation des systèmes d'intelligence artificielle générative publics limitée aux cas d'usage autorisés

18. Un organisme public doit encadrer de façon stricte l'utilisation des systèmes d'IAG publics[5] pour éviter tout usage abusif ou inapproprié. Ces systèmes publics autorisés doivent être identifiés au sein de l'organisme et ne peuvent être utilisés que dans des cas spécifiques et définis. Toute utilisation en dehors de ces cas d'usage autorisés est interdite.

19. L'encadrement visé à l'article 18 doit interdire au personnel d'utiliser des renseignements de nature confidentielle dans un système d'IAG public.

20. Un organisme public doit, afin de protéger la confidentialité et l'intégrité de ses données, prioriser l'utilisation des systèmes d'IAG privés sécurisés plutôt que des systèmes d'IAG publics.

SECTION VI
DISPOSITIONS DIVERSES

21. Un organisme public demeure tenu de respecter les obligations qui lui incombent en vertu de la loi et des textes d'application.

À cet égard, il peut consulter son service juridique afin de s'assurer qu'un système d'IAG et l'utilisation qui est envisagée soient conformes aux obligations applicables.

22. Le ministère de la Cybersécurité et du Numérique peut proposer des guides d'application évolutifs afin de soutenir les organismes publics dans la mise en œuvre de la présente indication d'application.

23. Un organisme public peut, à compter de la date d'entrée en vigueur de la présente indication d'application échelonner la mise en œuvre des mesures qui y sont prévues sur une période maximale de six mois suivant cette date.

[5] Système d'IAG public : toute version « grand public » gratuite ou non de systèmes d'IAG, comme les versions en ligne de Copilot (incluant Copilot Chat) et ChatGPT, accessible par le Web à l'extérieur de l'organisation, pour autant qu'elle ne soit pas interdite par celle-ci.

Ministère
de la Cybersécurité
et du Numérique
Québec

24. Malgré l'article 23, le dirigeant principal de l'information peut soustraire un organisme public, en tout ou en partie, à la mise en œuvre de la présente indication d'application, en raison d'une situation particulière et fixer les conditions alors applicables à un tel organisme.

25. La présente indication d'application abroge l'indication IA-RI-2025-001-OP relative à la suspension de l'utilisation des assistants virtuels s'appuyant sur l'intelligence artificielle générative.

Indications d'application liées (s'il y a lieu) :

- IA-SI-2025-001-OP « Interdictions d'utilisation au regard des assistants virtuels DeepSeek »;
- IA-SI-2023-001-OP « Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques »;
- IA-RI-2025-002-OP « Interdiction d'utilisation de la fonctionnalité « Inscription vocale et faciale » de l'application Microsoft Teams ».

Mots-clés : Intelligence artificielle │ Intelligence artificielle générative │ Données numériques gouvernementales │ Utilisation responsable

Date : 2025-12-05

ORIGINAL SIGNÉ
M. Stéphane Le Bouyonnec
Sous-ministre et dirigeant principal de l'information