Ministère de
la Sécurité publique
Québec

Direction de l'accès à l'information, des relations avec les citoyens et de la gestion documentaire

PAR COURRIEL

Québec, le 18 mars 2026

N/Réf. : 2026- 10393

OBJET: **Votre demande en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1)**

Madame,

Nous faisons suite à votre demande d'accès reçue le 30 janvier 2026, visant à obtenir les documents suivants *« du 1er janvier 2023 à aujourd'hui :*

1. copie de tout document ou fiche de breffage concernant l'utilisation des sites pornographiques par les employés de votre organisation, en particulier les hauts fonctionnaires;
2. les dépenses annuelles totales en papiers-mouchoirs pour cette même période ».

Concernant **le point 1,** nous vous informons que le ministère de la Sécurité publique (MSP) a repéré un document qui répond à votre demande et qui vous est accessible. Vous remarquerez, sur certaines des pages transmises, que nous avons élagué un renseignement personnel appartenant à un tiers en application des articles 53, 54 et 59 de la Loi sur l'accès.

Nous souhaitons toutefois porter à votre attention qu'une mise à jour de la directive encadrant l'utilisation d'Internet par le personnel est présentement en cours. En conséquence, la version transmise correspond à celle qui était en vigueur au moment du traitement de votre demande.

…2

2525, boulevard Laurier
Tour du Saint-Laurent, 10e étage
Québec (Québec) G1V 2L2
Téléphone : 418 646-6777, poste 11010
Télécopieur : 418 643-0275

En ce qui concerne **le point 2,** nous vous informons que le MSP n'a repéré aucun document dans la mesure où il ne tient aucun registre en lien avec les renseignements demandés. En vertu de l'article 1 de la Loi sur l'accès, nous sommes dans l'impossibilité de donner suite à votre demande. Pour être en mesure de répondre à cette dernière, le ministère devrait procéder à la compilation des informations demandées. Or, comme le droit d'accès ne porte que sur les documents dont la communication ne requiert ni calcul ni comparaison de renseignements, nous invoquons également l'article 15 de la Loi sur l'accès.

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous pouvez, en vertu de la section III du chapitre IV de cette loi (articles 135 et suivants), faire une demande de révision à l'égard de cette décision en vous adressant à la Commission d'accès à l'information dans les 30 jours suivant la date de la présente décision. À cet effet, vous trouverez joint à la présente le document intitulé Avis de recours.

Veuillez agréer, Madame, nos salutations distinguées.

Responsable de la Loi sur l'accès aux documents,

Original signé

Diane Gogoua

p. j. Articles de la loi et avis de recours en révision

Chapitre A-2.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

CHAPITRE I
APPLICATION ET INTERPRÉTATION

1. La présente loi s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers.

Elle s'applique quelle que soit la forme de ces documents: écrite, graphique, sonore, visuelle, informatisée ou autre.

1982, c. 30, a. 1.

CHAPITRE II
ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

SECTION I
DROIT D'ACCÈS

15. Le droit d'accès ne porte que sur les documents dont la communication ne requiert ni calcul, ni comparaison de renseignements.
1982, c. 30, a. 15.

CHAPITRE III
PROTECTION DES RENSEIGNEMENTS PERSONNELS

SECTION I
CARACTÈRE CONFIDENTIEL DES RENSEIGNEMENTS PERSONNELS

53. Les renseignements personnels sont confidentiels sauf dans les cas suivants:
1° la personne concernée par ces renseignements consent à leur divulgation; si cette personne est mineure, le consentement peut également être donné par le titulaire de l'autorité parentale;
2° ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.

1982, c. 30, a. 53; 1985, c. 30, a. 3; 1989, c. 54, a. 150; 1990, c. 57, a. 11; 2006, c. 22, a. 29.

54. Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.

1982, c. 30, a. 54; 2006, c. 22, a. 110

59. Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée.
Toutefois, il peut communiquer un tel renseignement sans le consentement de cette personne, dans les cas et aux strictes conditions qui suivent:

1° au procureur de cet organisme si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi que cet organisme est chargé d'appliquer, ou au Directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;

2° au procureur de cet organisme, ou au procureur général lorsqu'il agit comme procureur de cet organisme, si le renseignement est nécessaire aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe 1°;

3° à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;

4° à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;

5° à une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique;

6° *(paragraphe abrogé);*

7° *(paragraphe abrogé);*

8° à une personne ou à un organisme, conformément aux articles 61, 66, 67, 67.1, 67.2, 68 et 68.1;

9° à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement.

1982, c. 30, a. 59; 1983, c. 38, a. 55; 1984, c. 27, a. 1; 1985, c. 30, a. 5; 1987, c. 68, a. 5; 1990, c. 57, a. 13; 2006, c. 22, a. 32; 2005, c. 34, a. 37

AVIS DE RECOURS EN RÉVISION

Avis de recours à la suite d'une décision rendue par le ministère de la Sécurité publique en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Révision par la Commission d'accès à l'information

a) Pouvoir : l'article 135 de la Loi prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision. La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

Québec	**Montréal**
Bureau 2.36 525, boul. René-Lévesque Est Québec (Québec) G1R 5S9 Téléphone : 418 528-7741 Télécopieur : 418 529-3102	Bureau 900 2045, rue Stanley Montréal (Québec) H3A 2V4 Téléphone : 418 528-7741 Télécopieur : 418 529-3102

b) Motifs : les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais : les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

Directive ministérielle

sur l'utilisation du courriel, d'un collecticiel et des services d'Internet

Ministère de la Sécurité publique

Québec

TABLE DES MATIÈRES

CONTEXTE

Au cours des dernières années, les ressources informationnelles sont devenues indispensables à la prestation de la plupart des services aux citoyens, aux entreprises et aux partenaires du ministère de la Sécurité publique. Non seulement elles permettent d'augmenter la productivité, mais elles permettent d'améliorer la qualité des réalisations ministérielles par un accès illimité à des données à l'échelle planétaire. La modernisation de l'administration publique et la volonté gouvernementale de diversifier les modes de services publics en utilisant la prestation électronique de services imposent le recours aux nouvelles technologies de l'information et des télécommunications.

Le Conseil du trésor a adopté le 1er octobre 2002 la *Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique* (C.T. 198872). Celle-ci précise les attentes minimales auxquelles tout employé de la fonction publique doit répondre lors de l'utilisation d'un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet, au moyen de l'équipement gouvernemental mis à sa disposition ou au moyen de son équipement électronique.

Comme le Ministère a décidé d'ajouter des lignes directrices internes aux dispositions déjà contenues dans la directive adoptée par le Conseil du trésor, il est apparu opportun d'élaborer une directive ministérielle contenant les dispositions de la directive du Conseil du trésor ainsi que les lignes directrices et le partage des responsabilités spécifiques à la structure du Ministère. Ainsi, les employés n'auront qu'un seul document à lire pour connaître les dispositions qu'ils doivent respecter.

OBJECTIFS

Le Ministère doit offrir à tous ses utilisateurs un environnement sécuritaire et respectueux des droits collectifs et individuels. La directive a pour objectifs de :

- doter le personnel d'un cadre de référence régissant l'utilisation d'un accès ministériel au courriel, à un collecticiel et aux services d'Internet;
- déterminer le partage des responsabilités;
- s'assurer que les mesures de sécurité sont prises, notamment pour garantir la protection des renseignements personnels et des documents confidentiels détenus par le Ministère, qui circulent par voie électronique;
- sensibiliser le personnel aux risques inhérents à l'utilisation de ces ressources, notamment au fait que celle-ci laisse des traces permettant de déterminer l'ordinateur d'où provient le message.

CHAMP D'APPLICATION

Cette directive s'applique à tout le personnel du Ministère, à toute personne ou firme externe dûment autorisée à utiliser les services de courriel, d'un collecticiel et d'accès à Internet du Ministère et aux organismes relevant du ministre qui décideront de l'adopter.

La Direction générale de la Sûreté du Québec n'est pas visée par cette directive.

CADRE JURIDIQUE

Voici une liste non exhaustive des lois, règlements et directives sous-jacentes à l'élaboration des principes, dispositions et responsabilités contenus dans cette directive.

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1);

- *Loi sur les archives* (L.R.Q., c. A-21.1) et *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (R.R.Q., c. A-21.1, r. 1);

- *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1);

- *Charte des droits et libertés de la personne* (L.R.Q., c. C-12);

- *Loi sur la fonction publique* (L.R.Q., c. F-3.1.1) et *Règlement sur l'éthique et la discipline dans la fonction publique* (R.R.Q., c. F-3.1.1, r. 0.4);

- *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale* (CT 194055 du 23 novembre 1999);

- *Politique ministérielle de sécurité des actifs informationnels ;*

- *Charte canadienne des droits et liberté;*

- *Loi sur le droit d'auteur* (L.R.C. (1985), c. C-42);

- *Code criminel* (L.R.C. (1985), c. C-46).

PRINCIPES

Les logiciels de courriel, de collecticiel et d'accès à Internet sont mis à la disposition des employés autorisés pour :

- favoriser le développement des connaissances et des habiletés liées à l'utilisation des actifs informationnels;
- réaliser plus efficacement les tâches nécessaires à l'accomplissement de leurs fonctions;
- communiquer avec d'autres personnes autorisées et avec le public dans l'exercice de leurs fonctions.

Les principes sous-jacents à l'élaboration des dispositions contenues dans cette directive ministérielle sont les suivants :

- le respect des lois, des normes et des directives gouvernementales;
- le professionnalisme dans les communications électroniques;
- la protection des renseignements personnels et des documents confidentiels.

Le respect des lois, des normes et des directives gouvernementales

L'employé qui utilise un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet, respecte, outre les obligations prévues dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) :

- les règles et les pratiques en matière de sécurité de l'information et des renseignements personnels;
- la législation en matière de droits d'auteur;
- les règles d'utilisation de ces actifs informationnels en vigueur au Ministère;
- la Politique linguistique du ministère de la Sécurité publique dans ses communications écrites avec les intervenants externes;

Le calendrier de conservation du Ministère, établi en fonction de la *Loi sur les archives,* détermine les délais de conservation, les détenteurs principaux et le mode de disposition des documents, et précise ceux qui doivent être versés aux Archives nationales du Québec pour conservation permanente.

Le professionnalisme dans les communications électroniques

- Toute communication électronique doit être effectuée avec courtoisie et respect, conformément aux objectifs de qualité de services énoncés dans la *Déclaration de services aux citoyennes et aux citoyens du Ministère.* L'employé doit aussi fournir des réponses claires et précises. Pour ce faire, il utilise un langage simple et accessible à tous, et fournit de l'information concise, exacte et complète.

- L'expéditeur d'un courriel à un destinataire à l'extérieur du Ministère doit donner son nom véritable et complet. Outre son adresse électronique, il doit ajouter son titre, son unité administrative, son numéro de téléphone et son numéro de télécopieur.

- Tout courriel reçu par erreur, par exemple à un mauvais destinataire, doit être retourné à l'expéditeur, accompagné d'une note à cet effet, et être détruit par la suite.

- L'employé ne peut utiliser un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet pour :

  - harceler un employé de la fonction publique ou toute autre personne.

  - visionner, télécharger, copier, partager ou expédier des images ou des fichiers pornographiques, diffamatoires, offensants, haineux, violents, menaçants, racistes ou qui contreviennent à l'une des dispositions de la *Charte des droits et libertés de la personne (L.R.Q., c. C-12)* ainsi qu'à toute autre loi au Québec.

  - télécharger, partager, copier ou installer un logiciel sur l'équipement ministériel auquel il a accès sans une autorisation préalable.

  - utiliser à son profit les ressources technologiques, par exemple, envoyer des chaînes de lettres ou des messages publicitaires à des tiers, exprimer une opinion personnelle qui engagerait le Ministère, etc.

  - créer, expédier ou réexpédier tout message électronique ou fichier contenant un élément qui contrevient aux dispositions du cadre juridique ou qui est susceptible de nuire au fonctionnement de l'équipement mis à sa disposition ou du réseau ministériel auquel il est relié.

  - expédier un message à tout le personnel du Ministère, à moins d'avoir obtenu l'autorisation préalable de son gestionnaire.

La protection des renseignements personnels et des documents confidentiels

L'employé qui utilise un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet :

- respecte les dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* relatives à la collecte, à l'utilisation, à la communication, à la conservation, ou, selon le cas, à l'archivage ou à la destruction d'un renseignement personnel;

- ne transmet aucun renseignement personnel ou tout autre renseignement confidentiel non chiffré ou non protégé par un dispositif de sécurité éprouvé.

PARTAGE DES RESPONSABILITÉS

L'utilisateur

En plus de respecter les règles d'utilisation déjà stipulées dans la section **Principes**, l'utilisateur :

- Doit employer un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet à des fins pertinentes à la réalisation de ses fonctions. L'utilisation de ces accès à des fins personnelles constitue un privilège accordé par le Ministère. Cependant, cette utilisation doit se faire occasionnellement, se limiter au strict minimum, ne pas nuire aux activités professionnelles, n'impliquer aucun frais et ne causer aucun préjudice au Ministère ainsi qu'à son image.

- Doit éviter de déjouer les dispositifs de sécurité des systèmes informatiques, notamment en désactivant le logiciel antivirus ou en se servant du mot de passe, du code d'utilisateur ou du compte informatique d'un autre utilisateur.

- Doit choisir un mot de passe sécuritaire, par exemple une combinaison de chiffres, de lettres et de caractères spéciaux, et veiller à en préserver la confidentialité. Comme le mot de passe constitue la signature de l'utilisateur, il doit être réservé à son usage personnel. À ce titre, il engage sa responsabilité lorsqu'il accède aux systèmes d'information. L'utilisateur doit donc changer son mot de passe régulièrement ou immédiatement s'il le croit connu.

- Doit s'assurer que l'accès à son poste de travail est sécurisé par un écran de veille avec mot de passe lorsqu'il quitte temporairement son poste de travail. Il doit aussi utiliser un mot de passe pour protéger son courrier électronique et le rendre ainsi inaccessible à un tiers.

Le gestionnaire ou son représentant désigné

- Décide s'il est opportun de donner à un membre de son personnel un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet. Ce privilège est susceptible d'être révoqué en tout temps, en conformité avec la présente directive.

- Doit sensibiliser son personnel aux dispositions de la directive et aux modalités de sa mise en œuvre.

- Doit s'assurer, sous réserve de la mesure d'exception, que les ressources de l'inforoute sont utilisées en conformité avec les principes directeurs et les lignes de conduite de la présente directive, dans le cadre des tâches et responsabilités confiées aux personnes relevant de sa responsabilité.

- Doit s'assurer que les personnes qui ne font pas partie du personnel et qui se sont vu confier un mandat par le Ministère ont accès aux renseignements personnels ou confidentiels uniquement lorsque la réalisation de leurs activités l'exige. Une entente écrite devrait spécifier des clauses de confidentialité, en conformité avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

- Doit aviser la Direction des technologies de l'information et des acquisitions de toute modification à apporter aux droits d'accès du personnel de son unité administrative.

- Doit faire la demande d'un logiciel de chiffrement ou de tout autre dispositif de sécurité éprouvé auprès de la Direction des technologies de l'information et des acquisitions lorsque le personnel de son unité administrative transmet ou reçoit par courriel des renseignements personnels et des documents confidentiels détenus par le Ministère.

La Direction des technologies de l'information et des acquisitions

- Doit fournir les logiciels de courriel, de collecticiel et d'accès à Internet, les entretient et en assure la sécurité.

- Doit mettre à la disposition des utilisateurs qui en font la demande un logiciel ou tout autre dispositif de sécurité éprouvé permettant le chiffrement et la protection des messages contenant des renseignements personnels.

- Doit s'assurer que les postes de travail (ordinateurs de table ou portables) sont équipés d'un logiciel antivirus à jour.

- Doit mettre en place les dispositifs nécessaires aux vérifications énoncées dans la directive.

- Évalue régulièrement les vulnérabilités et les risques susceptibles de nuire aux ressources technologiques constituant le réseau étendu ministériel.

Le responsable de la gestion de l'information documentaire

- Doit établir et diffuser les règles de classification et de conservation des messages électroniques avec ou sans documents attachés et veiller au respect de leur application en conformité avec les lois, règlements, directives, normes et procédures de gestion de l'information.

Le sous-ministre ou dirigeant d'organisme

- Est responsable de l'application de la présente directive.

- Peut exceptionnellement autoriser un membre de son personnel à utiliser un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet selon des conditions autres que celles prévues dans la directive si la nature du travail l'exige. Cette autorisation peut être révoquée en tout temps.

DROIT DE REGARD

Le sous-ministre ou le dirigeant d'organisme a droit de regard sur l'utilisation des actifs informationnels par les employés. Ainsi, il peut avoir accès à toute information consignée sur son équipement électronique, au moyen du courriel, d'un collecticiel ou des services d'Internet ou par tout autre moyen.

Lorsque les circonstances le justifient, le sous-ministre ou le dirigeant d'organisme peut appliquer des mesures de gestion sur les actifs informationnels du Ministère, notamment en soumettant un employé à une vérification particulière de l'utilisation qu'il fait de ceux-ci ou de l'information contenue dans les fichiers personnels de ce dernier.

Le sous-ministre ou le dirigeant d'organisme doit effectuer des vérifications régulières de l'utilisation d'un accès gouvernemental au courriel, à un collecticiel ou aux services d'Internet pour des motifs opérationnels et procéder à l'analyse de leurs résultats.

Ce droit de regard sera exercé conformément à la loi, notamment à l'égard de la protection de la vie privée, des renseignements personnels et confidentiels.

MESURE D'EXCEPTION

Toute personne assujettie à la présente directive qui a une raison valable de déroger aux obligations, principes ou lignes de conduite qui y sont prévus doit formuler une demande écrite à son supérieur et obtenir son autorisation écrite.

SANCTION

Le sous-ministre ou le dirigeant d'organisme ou son représentant désigné détermine, selon la nature ou la gravité du cas, s'il est opportun d'appliquer une sanction disciplinaire ou de prendre une mesure administrative lorsqu'un membre contrevient à la directive ou à la loi.

APPROBATION

La présente directive entre en vigueur le jour de son approbation par le sous-ministre.

[redacted] 2004-02-02

LUC CRÉPEAULT, sous-ministre — Date

ANNEXE 1 - LEXIQUE

Chiffrement	Opération par laquelle est substitué à un texte en clair un texte inintelligible et inexploitable pour quiconque ne possédant pas la clé pour le ramener à sa forme initiale.
Collecticiel	Logiciel qui permet à des utilisateurs reliés par un réseau de travailler en collaboration sur un projet.
Courriel	Service de correspondance sous forme d'échange de messages électroniques, à travers un réseau informatique. Par extension, message transmis par un utilisateur vers un ou plusieurs destinataires, d'ordinateur à ordinateur, par l'intermédiaire d'un réseau informatique.
Fichier	Ensemble d'informations consignées et stockées comme une entité unique et spécifique sur un support de stockage.
Internet	Réseau informatique mondial constitué de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.
Renseignement personnel	Information de caractère non public concernant une personne physique et permettant de l'identifier, directement ou indirectement.
Renseignement confidentiel	Renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations inter-gouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs secrets industriels, l'administration de la justice, la sécurité publique, les décisions administratives ou politiques et la vérification.
Réseau	Système de transmission interconnectant les clients et les services ainsi que le matériel et les logiciels afférents.