MÉMOIRE AU CONSEIL DES MINISTRES **GOUVERNEMENT DU QUÉBEC**

DE : Madame Sonia LeBel — Le 23 novembre 2021
Ministre responsable de l'Administration gouvernementale
et présidente du Conseil du trésor

Monsieur Éric Caire
Ministre délégué à la Transformation numérique gouvernementale

---

TITRE : Décret concernant la Directive gouvernementale sur la sécurité de l'information

---

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

La Stratégie de transformation numérique gouvernementale 2019-2023 et la Politique gouvernementale de cybersécurité (ci-après la Politique) façonnent un environnement où les attentes envers l'Administration publique sont élevées en matière de sécurité de l'information. Non seulement les dernières années ont été marquées par de nombreux incidents de sécurité de l'information aux conséquences importantes partout dans le monde, dont au Québec, mais les changements opérés par une offre numérique plus intégrée des prestations de services sont irrémédiablement accompagnés d'enjeux de sécurité de l'information qui nécessitent d'être pris en charge. Parmi ces enjeux, pensons notamment à la valorisation des données de manière sécuritaire et à la protection des renseignements des citoyens pour le respect de leur vie privée.

La Politique a été adoptée par le gouvernement du Québec en mars 2020. Elle vise à rehausser la résilience et la cyberprotection de l'Administration gouvernementale, à accroître le niveau de maturité des organismes publics en matière de cybersécurité et à maintenir la confiance des citoyens au regard de la prise en charge de la cybersécurité au gouvernement du Québec. Les mesures clés qui l'accompagnent, annoncées en mai 2020, ont été définies afin d'assurer sa mise en œuvre. Parmi celles-ci, la mesure 1.1 prévoit de « renforcer l'encadrement de la sécurité de l'information gouvernementale ».

En novembre 2019, le Centre gouvernemental de cyberdéfense a été créé au sein du Secrétariat du Conseil du trésor, et des actions se sont depuis mises en œuvre pour déployer un réseau gouvernemental de cyberdéfense, en concordance avec l'objectif 5 de la Politique. Jusqu'à présent, la communauté gouvernementale s'implique fortement à constituer et à participer à ce réseau. Toutefois, le modèle de gouvernance définit par la Directive sur la sécurité de l'information gouvernementale actuellement en vigueur ne leur confère aucune légitimité d'action.

En juin 2021, la Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives a été sanctionnée. Elle introduit à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du

gouvernement (chapitre G-1.03) (ci-après la Loi sur les ressources informationnelles) de nouvelles responsabilités au dirigeant principal de l'information et aux dirigeants de l'information en matière de sécurité de l'information, et ce, afin de renforcer la structure de gouvernance à l'échelle gouvernementale. Toutefois, l'intégration des organismes publics à cette structure n'est pas explicitement présente dans la Loi sur les ressources informationnelles.

Ainsi, une opportunité se présente pour optimiser la gouvernance de la sécurité de l'information gouvernementale. C'est pourquoi la révision de la Directive sur la sécurité de l'information gouvernementale s'avère essentielle et qu'il est proposé de la remplacer par la Directive gouvernementale sur la sécurité de l'information.

2- Raison d'être de l'intervention

Un rapport d'évaluation de la directive actuellement en vigueur été déposé au Conseil du trésor en octobre 2019. Ce rapport présente des résultats positifs, notamment en ce qui concerne le taux de conformité aux exigences de sécurité de l'information par les organismes publics, mais dévoile certaines lacunes. Le maintien en vigueur de la directive actuelle pourrait avoir pour effet d'exacerber les lacunes observées et de creuser davantage l'écart avec la situation souhaitée.

En outre, ce scénario aurait comme conséquence de maintenir en place une structure de gouvernance qui n'enchâsserait pas dans le corpus législatif l'existence du Centre gouvernemental de cyberdéfense, des centres opérationnels de cyberdéfense et du Réseau gouvernemental de cyberdéfense, ce qui ne leur permettait pas d'assumer adéquatement leurs responsabilités en matière de prévention et de prise en charge des événements de sécurité de l'information. Force est de constater que le besoin se fait sentir de mettre en place une chaîne de commandement plus efficace, de mieux structurer les rôles et les responsabilités des intervenants en sécurité de l'information, et de se donner les moyens de réagir plus efficacement en cas d'événements de sécurité de l'information.

Enfin, la directive actuellement en vigueur ne reflète pas les changements législatifs amenés par la Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives; il est donc nécessaire de la faire évoluer.

3- Objectifs poursuivis

Le projet de directive annexé au présent mémoire a pour objet d'assurer adéquatement une prise en charge globale de la sécurité de l'information qu'un organisme public détient dans l'exercice de ses fonctions, que la conservation de cette information soit assurée par lui-même ou par un tiers.

Par la mise en place d'un encadrement optimal et par l'établissement de règles, elle complète les dispositions de la Loi sur les ressources informationnelles, en cohérence avec la Politique gouvernementale afin de viser une Administration publique résiliente et cyberprotégée à l'ère du numérique.

Elle énonce les principes directeurs devant être appliqués et prévoit une gouvernance de la sécurité de l'information qui repose sur une structure de coordination, de concertation et de soutien aux organismes publics en telle matière.

Elle prévoit des règles applicables aux organismes publics en vue d'assurer, en matière de sécurité de l'information, la confidentialité, l'intégrité et la disponibilité de l'information tout au long de son cycle de vie, et afin de couvrir des enjeux particuliers en telle matière.

4- Proposition

Modèle de gouvernance de la sécurité de l'information gouvernementale

Le projet de directive propose aux organismes publics visés à l'article 2 de la Loi sur les ressources informationnelles, une structure de gouvernance de la sécurité de l'information à trois niveaux d'autorité. Alors que la Loi sur les ressources informationnelles confie au dirigeant principal de l'information la fonction de chef gouvernemental de la sécurité de l'information et aux dirigeants de l'information celle de chefs délégués de la sécurité de l'information, le projet de directive crée, au sein de chaque organisme public, la fonction de chef de la sécurité de l'information organisationnelle, désigné par le sous-ministre ou le dirigeant d'un organisme public. Pour les ministères, cette fonction est attribuée *de facto* au chef délégué de la sécurité de l'information du portefeuille ministériel concerné.

Ce découpage en trois niveaux crée des liens fonctionnels (un lien fonctionnel étant « un rapport entre deux personnes qui, selon le contexte, permet à l'une d'entre elles de formuler un ordre à l'autre, sans qu'il existe un lien hiérarchique entre ces personnes ») entre les niveaux d'autorité, ce qui favorise une collaboration agile et transparente pour réagir efficacement, en cas d'événements de sécurité de l'information. Ces trois fonctions couvrent les volets stratégiques, tactiques et opérationnels de la sécurité de l'information, et ce, afin d'assurer une prise en charge globale de la sécurité de l'information gouvernementale.

De plus, la constitution du Réseau gouvernemental de cyberdéfense est précisée. Le Centre gouvernemental de cyberdéfense et les centres opérationnels de cyberdéfense sont officiellement intégrés dans le modèle de gouvernance par ce projet de directive. Également, des fonctions de responsable gouvernemental de cyberdéfense et de responsables opérationnels de cyberdéfense sont ajoutées afin d'appuyer le déploiement du Réseau gouvernemental de cyberdéfense.

Activités découlant des responsabilités définies dans la Loi sur les ressources informationnelles

Le projet de directive vient préciser les activités découlant des responsabilités attribuées au chef gouvernemental de la sécurité de l'information et aux chefs délégués de la sécurité de l'information dans la Loi sur les ressources informationnelles. Le chef gouvernemental de la sécurité de l'information devra notamment définir des processus gouvernementaux normalisés afin d'harmoniser les pratiques de sécurité de l'information au sein de l'Administration publique. Les chefs délégués de la sécurité de l'information devront notamment diriger le centre opérationnel de cyberdéfense auxquels ils se rattachent, l'opérationnaliser et faire évoluer son offre de services, en plus de mettre en œuvre toute action requise pour la prise en charge d'un événement de sécurité.

Nouvelles obligations aux organismes publics

Le projet de directive impose aux organismes publics d'assurer la gestion des événements de sécurité, de déployer les mesures et les processus afférents en matière de sécurité de l'information et d'en assurer le suivi de la mise en œuvre. Il stipule également que les organismes publics doivent tenir un registre des événements de sécurité de l'information et en transmettre une copie au chef gouvernemental de la sécurité de l'information, sur demande de celui-ci.

Elle précise également que les organismes publics devront respecter les indications d'application formulées par le chef gouvernemental de la sécurité de l'information ou les indications d'application particulières formulées par le chef délégué de la sécurité de l'information.

Afin de s'assurer que le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec prennent les moyens nécessaires pour que les acquisitions en bien ou en services effectuées pour le compte des organismes publics répondent aux besoins de sécurité de l'information exprimés par ces derniers, des obligations leur sont ajoutées. Pour Infrastructures technologiques Québec, les obligations sont liées à son service de courtier en infonuagique. En effet, la prise en compte des enjeux de sécurité de l'information dans les pratiques de gestion des infrastructures technologiques et dans les pratiques en gestion contractuelle est incontournable. Conséquemment, la valeur de l'information, l'évolution rapide des technologies et la présence d'information sur une multitude d'objets d'utilisation quotidienne exigent de plus en plus de connaissances pointues et une rigueur irréprochable. S'ajoutent à ce contexte l'émergence de l'intelligence artificielle et l'Internet des objets, deux nouveaux domaines d'expertise à considérer.

Finalement, des obligations particulières sont prévues pour les organismes publics fournisseurs de services communs de sécurité de l'information, incluant Infrastructures technologiques Québec, et ce, afin d'assurer que le partage des responsabilités soit clair et précis entre le fournisseur du service commun et les utilisateurs du service et que les mesures de sécurité répondent adéquatement aux enjeux et aux risques de sécurité de l'information afférents de chacune des parties.

5- Autre option

Bien qu'une Directive sur la sécurité de l'information gouvernementale soit déjà en vigueur, celle-ci ne tient pas compte des nombreux changements survenus dans la gouvernance en sécurité de l'information gouvernementale depuis 2014, et ne tient pas compte de plusieurs documents phares, comme la Politique gouvernementale de cybersécurité, la Stratégie de transformation numérique gouvernementale 2019-2023 ou la Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives, sanctionnée en juin 2021. Ainsi, la seule option était de réviser la directive actuellement en vigueur.

6- Évaluation intégrée des incidences

Incidences sur les citoyens

L'adoption et la mise en œuvre de ce projet de directive, avec l'importance que doivent accorder les organismes publics à la sécurité de l'information, notamment à la protection des renseignements personnels, devraient contribuer à rehausser le niveau de confiance des citoyens envers la sécurité des programmes et des services gouvernementaux. Par ailleurs, considérant que l'utilisation par les citoyens services numériques est un incontournable à la transformation numérique de l'Administration publique, la sécurité est un pilier de cette transformation.

Incidences économiques

Le rehaussement des exigences en sécurité de l'information et l'implantation d'une meilleure structure de gouvernance permettant aux organismes publics de mieux se prémunir contre les risques de sécurité pourraient augmenter l'efficience en matière de sécurité de l'information et améliorer la performance de ces derniers. Considérant que les incidents de sécurité sont généralement coûteux, imprévisibles et qu'ils peuvent nuire de façon importante à la prestation de services aux citoyens, il est permis de croire qu'une meilleure protection en amont constituerait un meilleur investissement que les sommes engagées en réaction à un incident, à condition de s'assurer que les mesures mises en place induisent une diminution de la survenance de ces incidents et des impacts en découlant.

Incidences sur la société

Le gouvernement du Québec se doit d'être exemplaire en matière de sécurité de l'information. En effet, l'information qu'il détient est sensible, et les prestations de services qu'il supporte sont essentielles pour les citoyens; le moindre manquement en matière de sécurité de l'information peut entraîner des préjudices sérieux, aussi bien pour les citoyens que pour l'Administration publique. Ainsi, le fait de s'assurer du respect des obligations en matière de sécurité de l'information par les organismes publics et d'en faire le suivi de la performance à l'échelle gouvernementale devrait permettre de renforcer la sécurité à l'échelle gouvernementale et de faire de l'Administration publique un modèle en la matière. Il est aussi permis de croire que les interactions entre l'Administration publique et tous ses

partenaires seront facilitées grâce au rehaussement de la sécurité de l'information gouvernementale et de la confiance accrue qui en découlent.

7- Consultation entre les ministères et avec d'autres parties prenantes

Les responsables organisationnels de la sécurité de l'information ont été consultés en août 2019 pour recueillir leurs préoccupations en lien avec la révision de la Directive sur la sécurité de l'information gouvernementale, alors qu'ils ont pu échanger sur les changements proposés à la structure de gouvernance en décembre 2020

Depuis juin 2020, les dirigeants de l'information ont été rencontrés et sont impliqués dans le déploiement des centres opérationnels de cyberdéfense de façon volontaire. Également, certains d'entre eux ont été consultés en juin 2021, par l'entremise du sous-comité sécurité de l'information et données gouvernementales, afin de recueillir leurs commentaires et suggestions sur le projet de directive. Les commentaires qui ont été formulés à l'occasion de ces consultations ont été pris en compte dans la présente proposition.

Finalement, le projet de directive a été recommandé par le comité de gouvernance en ressources informationnelles le 22 septembre 2021.

8- Mise en œuvre, suivi et évaluation

Le projet de directive prévoit que le chef gouvernemental de la sécurité de l'information doit, au plus tard cinq années après la date d'entrée en vigueur de la Directive et par la suite, tous les cinq ans, faire au Conseil du trésor un rapport sur l'application de la présente directive et sur l'opportunité de maintenir ou de modifier ses dispositions.

9- Implications financières

La mise en œuvre du projet de directive et la réalisation des obligations qui y sont prévues devront être assumées à même les budgets alloués aux organismes publics.

Une telle directive ayant pour objet d'assurer une prise en charge globale de la sécurité de l'information et d'assurer la mise en place d'un modèle de gouvernance fort et concerté au sein de l'Administration publique, une réallocation des priorités de dépenses pourrait être nécessaire au sein de certains organismes publics.

Pour le soutien au déploiement du Réseau gouvernemental de cyberdéfense, des sommes additionnelles sont déjà pourvues par l'adoption de la Politique.

10- Analyse comparative

Le projet de directive accompagnant le présent mémoire prend appui sur une analyse de différentes initiatives d'autres administrations gouvernementales à l'échelle mondiale. Ainsi, les rôles proposés par la nouvelle structure de gouvernance sont alignés sur les meilleurs modèles et tiennent compte des tendances actuelles. Les exigences proposées s'inspirent des bonnes pratiques de sécurité reconnues mondialement. L'analyse comparative a également mis en lumière tous les éléments importants à couvrir en ce qui concerne les obligations de sécurité de l'information, notamment en se basant sur le rapport d'audit interne du 30 avril 2020 du ministère de la Sécurité publique du Canada. Pareillement, le modèle préconisé dans le déploiement du réseau gouvernemental de cyberdéfense est basé sur le *National Institute of Standards and Technology* (NIST), une référence mondiale en matière de cyberdéfense.

La ministre responsable de
l'Administration gouvernementale
et présidente du Conseil du trésor,

SONIA LEBEL

Le ministre délégué à la
Transformation numérique
gouvernementale,

ÉRIC CAIRE