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

DE : Madame Sonia LeBel — Le 19 octobre 2021
Ministre responsable de l'Administration gouvernementale et présidente du Conseil du trésor

Monsieur Éric Caire
Ministre délégué à la Transformation numérique gouvernementale

---

TITRE : Projet de loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions

---

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

La transformation numérique est une tendance mondiale tant dans le secteur public que privé. Pour les administrations publiques, elle permet notamment d'améliorer l'accès aux services pour les citoyens et les entreprises, de simplifier, voire même d'éliminer les formalités, d'augmenter l'efficacité de la gestion des programmes et d'en réduire les coûts administratifs et de pallier la rareté de main-d'œuvre.

Depuis 2019, le gouvernement du Québec a jeté les assises de sa transformation numérique en rendant publiques sa Stratégie de transformation numérique gouvernementale 2019-2023 ainsi que sa Politique gouvernementale de cybersécurité, en instituant Infrastructures technologiques Québec et en adoptant la Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021-2026.

Le passage au monde numérique a été accéléré, pour tous les secteurs de l'économie, par les mesures sanitaires mises en place pour contrôler la propagation de la COVID-19. En effet, depuis mars 2020, le Québec, à l'instar de tous les autres États du monde, a dû recourir aux technologies du numérique pour éviter des bris de services qui auraient eu pour conséquences de fragiliser davantage l'économie. Les organismes publics et les entreprises privées ont ainsi accéléré leur transformation numérique afin de livrer leur prestation de services. Ce phénomène s'est traduit par l'implantation d'outils nécessaires afin de soutenir le télétravail du personnel ou le développement de services en ligne, augmentant ainsi de façon exponentielle les risques de cyberattaques.

Pour l'administration publique québécoise qui multiplie les plateformes transactionnelles et les outils numériques, la protection contre les cyberattaques devient non seulement une priorité, mais une nécessité considérant l'importance et la sensibilité des données numériques qu'elle détient et utilise.

Les cyberattaques, la nouvelle pandémie[1]

En novembre 2020, le Centre canadien pour la cybersécurité publiait son *Évaluation des cybermenaces nationales 2020* laquelle met en évidence les risques de cybermenaces touchant la sécurité de l'information, les infrastructures technologiques et, de manière plus générale, l'ensemble de la population.

Le rapport met notamment en lumière les constats suivants :

- le nombre d'auteurs de cybermenaces est en hausse et ceux-ci deviennent de plus en plus sophistiqués;
- la cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes;
- les activités malveillantes dirigées contre le Canada continueront fort probablement de cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles;
- il est fort probable que des auteurs de cybermenaces parrainés par des États cherchent à développer des moyens pour perturber les infrastructures essentielles du Canada, comme l'approvisionnement en électricité, pour atteindre leurs buts;
- les auteurs de cybermenaces continueront probablement de mener des activités d'espionnage industriel contre les entreprises, le milieu universitaire et les gouvernements du Canada afin de voler la propriété intellectuelle et des renseignements canadiens de nature exclusive.

Le Québec, tout comme les autres provinces canadiennes, ne fait pas exception et est lui aussi victime de nombreuses attaques. Le Canada étant un proche allié des États-Unis, il représente une cible de choix pour des attaques indirectes envers eux. Uniquement depuis la dernière année, des entreprises ou des organismes québécois issus des secteurs névralgiques de l'activité sociale ou économique ont fait l'objet d'actes malveillants. Parmi les événements ayant été médiatisés, on retrouve ceux ayant touché les entreprises du transport en commun (la Société de transport de Montréal), les centres hospitaliers (Centre intégré de santé et de services sociaux du Centre-Ouest-de-l'Île-de-Montréal), les établissements d'enseignement (Cégep de Saint-Félicien), les entreprises alimentaires (Groupe Olymel, Nutrinor), les compagnies d'assurance (Promutuel), le monde municipal (Ville de Châteauguay), les services de garde (La Place 0-5) et les organismes du milieu culturel (Bibliothèque et Archives nationales du Québec). Le constat est simple : aucun secteur d'activité n'est à l'abri d'une cyberattaque.

Aux États-Unis, des cyberpirates ont réussi à perturber les activités de transport énergétique (Colonial Pipeline) causant des pénuries en carburant, l'approvisionnement en eau dans certains états américains (Floride, Californie, Kansas) et le commerce de détail et les fonctions de paiement électroniques (Société Kaseya).

Les cyberattaques de ce genre pourraient, selon la firme spécialisée *Cybersecurity ventures* (le plus important groupe de recherche privé au monde en sécurité informatique) être plus

[1] L'Express, n° 3660, 26 août au 1er septembre 2021, *Hôpitaux, centrales nucléaires, entreprises : Cyberattaques, la nouvelle pandémie*, pages 14-20

fréquentes et importantes au cours des prochaines années. Elle estime que leurs coûts pourraient atteindre 13 300 milliards de dollars en 2025. On parle alors des coûts estimés pour le vol de propriété intellectuelle, les fraudes financières auprès des banques, des entreprises et des particuliers, le vol de données confidentielles ainsi que la destruction de données sensibles.

Selon un récent rapport publié en 2021 par IBM, de 2019-2020 à 2020-2021, le coût moyen d'un vol de données à la suite d'une cyberattaque a augmenté de 10 %, passant de 3,86 M$ à 4,24 M$[2].

Les cyberattaques étant lucratives pour les pirates et coûteuses pour les victimes, tout laisse à croire que leur nombre n'est pas près de diminuer. Les bénéfices possibles, comme lorsque des rançongiciels sont utilisés, sont souvent supérieurs aux risques pris par les pirates informatiques.

La gouvernance actuelle des ressources informationnelles

Le cadre normatif régissant les ressources informationnelles de l'administration publique a considérablement évolué au cours des deux dernières années :

- La Loi favorisant la transformation numérique de l'administration publique (chapitre T-11.003) – sanctionnée le 10 octobre 2019

  Cette loi vise à soutenir la réalisation de projets importants de transformation numérique, dont ceux d'intérêt gouvernemental, notamment en facilitant et en balisant l'utilisation et la communication de renseignements personnels si cette communication était nécessaire à la réalisation d'un projet en ressources informationnelles.

- La Loi visant principalement à instituer le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec (LQ 2020, chapitre 2) – 21 février 2020

  Cette loi vise notamment à améliorer la performance de l'État et à rencontrer les cibles prévues au cadre financier. En matière de gestion des technologies, elle visait à dégager les organismes publics de la gestion des infrastructures technologiques et des systèmes de soutien administratifs en les confiant à Infrastructures technologiques Québec (ITQ), une nouvelle entité en remplacement du Centre de services partagés du Québec.

- 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 (LQ 2021, chapitre 22) – 10 juin 2021

  Cette loi vise à adapter le cadre législatif québécois à l'évolution de l'univers numérique et à renforcer les moyens permettant de contrer les cyberattaques ainsi qu'à mieux gérer les données numériques gouvernementales.

[2] IBM Security. « Cost of a Data Breach Report 2021 ». https://www.ibm.com/security/data-breach

Ces travaux législatifs visaient l'atteinte d'un objectif commun, soit de renforcer le cadre normatif en ressources informationnelles de façon notable et ainsi pouvoir entreprendre les ajustements à la structure administrative gouvernementale.

Par ailleurs, la sanction en septembre 2021 de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels introduit à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.01) des dispositions qui permettent de créer un meilleur encadrement applicable aux renseignements personnels.

En vertu de la Loi sur les ressources informationnelles, la gouvernance des ressources informationnelles à l'échelle de l'administration publique est sous la responsabilité du dirigeant principal de l'information (DPI) qui relève du Secrétariat du Conseil du trésor. Le Centre québécois d'excellence numérique et le Centre gouvernemental de cyberdéfense (créés en 2019) sont sous sa responsabilité, de même que l'élaboration des normes et politiques en matière de ressources informationnelles. En vertu de la réglementation en vigueur, plusieurs décisions sont également prises en cette matière par le Conseil du trésor.

Quant à ITQ, il a pour mission, dans le respect des orientations du Conseil du trésor, de fournir aux organismes publics des services en infrastructures technologiques et en systèmes de soutien communs permettant notamment de soutenir de tels organismes dans l'exercice de leurs fonctions et dans leur prestation de services afin de favoriser leur transformation numérique. ITQ agit également à titre de courtier infonuagique.

Le DPI et ITQ sont responsables du développement et de la mise en œuvre de plusieurs projets importants liés à la transformation numérique de l'administration publique, dont deux désignés d'intérêt gouvernemental par le Conseil du trésor soit le Service québécois d'identité numérique (SQIN) et le Programme de consolidation des centres de traitement informatique (CCTI).

En ce qui concerne la coordination des activités de soutien et de protection des citoyens et des entreprises du Québec contre les cyberattaques, cette responsabilité n'est actuellement pas attribuée à un portefeuille ministériel.

Les ressources informationnelles en chiffres

Pour le gouvernement du Québec, les ressources informationnelles c'est plus de 4,3 G$ de dépenses planifiées pour l'exercice financier 2021-2022, 3 992 systèmes informatiques et plus de 200 projets en exécution. Au Plan québécois des infrastructures 2021-2031, secteur « ressources informationnelles », c'est 7,2 G$ qui sont planifiés, dont 848 M$ pour l'exercice financier 2021-2022.

En décembre 2020, 22 868 ressources travaillaient au sein de l'administration publique en ressources informationnelles, soit 18 538 internes et 4 330 externes. À cette même date, 1 960 postes étaient vacants.

2- Raison d'être de l'intervention

La structure administrative actuelle ne favorise pas une utilisation optimale des ressources dédiées à l'application de la Loi sur les ressources informationnelles et à la Loi sur Infrastructures technologiques Québec (chapitre I-8.4). La gestion des ressources informationnelles, incluant les activités liées à la cybersécurité, est désormais un champ d'intervention de l'État à part entière. Il est donc nécessaire, dans un souci de performance et de saine gestion des fonds publics, de regrouper au sein d'une même entité l'élaboration des politiques et des orientations ainsi que la conduite des opérations.

La création d'un ministère constitue une réponse formulée aux enjeux soulevés lors de l'étude de 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, voulant que :

- les organismes publics ont un niveau de maturité variable en matière de cybersécurité, rendant le gouvernement vulnérable à des cyberattaques;
- les travaux en matière de transformation numérique doivent se poursuivre pour donner une nouvelle impulsion à la transformation numérique des organismes publics et, ainsi, de l'administration publique;
- les priorités gouvernementales en matière d'investissements en RI sont encore mal définies, de sorte que près de 500 projets en ressources informationnelles sont prévus au PQI-RI par les organismes des différents portefeuilles ministériels sans qu'ils ne soient nécessairement alignés directement sur les priorités du gouvernement ou coordonnés entre eux.

Bien que le DPI et ITQ collaborent déjà en matière de rehaussement du niveau de sécurité des actifs de l'État et de la transformation numérique, le regroupement des deux instances permettrait d'accroître la synergie nécessaire pour faciliter la poursuite des travaux, évitant ainsi du développement en silo permettant d'atteindre plus rapidement les objectifs du gouvernement. La mise en place de fondations sera facilitée, tant au niveau de la gouvernance que des opérations.

3- Objectifs poursuivis

L'objectif de la proposition est de regrouper au sein d'une même entité les activités d'élaboration des politiques et des orientations en matière de ressources informationnelles, incluant la cybersécurité, ainsi que les activités de conception, de réalisation et d'exploitation des projets numériques et technologiques communs ou à portée gouvernementale.

Considérant la rareté de la main-d'œuvre possédant une expertise spécialisée en ressources informationnelles, le regroupement des experts des deux entités ciblées facilitera la mise en commun et le partage des connaissances.

En plus d'améliorer la fluidité du processus décisionnel lié à la mise en œuvre des activités liées aux ressources informationnelles, la proposition a également pour objectifs une

meilleure gestion de ces ressources ainsi que la livraison des mesures d'économies fixées par le gouvernement.

La proposition vise également à :

- optimiser la conduite des projets en ressources informationnelles;
- améliorer les bénéfices générés par la conduite de ceux-ci;
- concourir à l'augmentation de la performance de l'État, notamment par la sélection des meilleurs investissements;
- accélérer la transformation numérique de l'État;
- améliorer la qualité des services destinés aux citoyens et aux entreprises;
- structurer le commandement en matière de cybersécurité.

4- Proposition

Il est proposé de créer le ministère de la Cybersécurité et du Numérique, qui serait composé du personnel du Sous-secrétariat du dirigeant principal de l'information et de la transformation numérique et de celui d'Infrastructures technologiques Québec.

Ce nouveau ministère se verrait attribuer une fonction ministérielle dédiée à la cybersécurité et au numérique tout en reprenant les responsabilités actuellement assumées par le DPI et ITQ. Ainsi, il sera possible de simplifier les structures administratives, de rendre les processus décisionnels plus rapides et d'optimiser l'utilisation des ressources spécialisées affectées à ces domaines d'activités de pointe. Ce ministère serait non seulement responsable de la cybersécurité à l'échelle de l'administration publique, mais il aurait aussi pour mission de coordonner les initiatives des organismes publics pouvant soutenir et mieux protéger la société québécoise contre les cyberattaques, en collaboration avec des acteurs clés dont le ministère de la Sécurité publique et les corps policiers, le gouvernement du Canada et les gouvernements provinciaux, les gouvernements des autres juridictions sans oublier les grandes entreprises du gouvernement, dont Hydro-Québec et la Caisse de dépôt et placement du Québec.

Responsabilités générales du ministre

Le projet de loi propose la création du ministère et fixe les responsabilités générales du ministre qui le dirigerait :

- il aurait pour mission d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique;
- il proposerait au gouvernement les grandes orientations en ces domaines, déterminerait les secteurs d'activités dans lesquels il entendrait agir en priorité et conseillerait le gouvernement et les organismes publics;
- il proposerait également au gouvernement des mesures en vue d'accroître l'efficacité de la lutte contre les cyberattaques et les cybermenaces au Québec;

— il devrait établir des objectifs et élaborer des politiques, des stratégies et des programmes propres à assurer l'accomplissement de sa mission. Il dirigerait, coordonnerait et surveillerait l'application de ces objectifs, politiques, stratégies et programmes.
— il pourrait, dans les domaines de la cybersécurité et du numérique, accorder des subventions et, avec l'autorisation du gouvernement, accorder toute autre forme d'aide financière.

Fonctions et pouvoirs du ministre

À l'égard des organismes publics visés à l'article 2 de la Loi sur les ressources informationnelles, lesquels forment l'administration publique, les fonctions et pouvoirs du ministre consisteraient à :

— développer un ensemble de moyens visant à offrir aux citoyens et aux entreprises une prestation de services numériques de qualité par les ministères et les organismes;
— veiller à l'utilisation optimale des technologies du numérique dans la prestation des services publics;
— assurer le développement, l'implantation et le déploiement de l'administration publique numérique de même que la promotion et la mise en œuvre de toute mesure favorisant l'adaptation à cette fin des services publics;
— assurer la mise en œuvre d'une stratégie visant la transformation numérique de l'administration publique, incluant, le cas échéant, la mise en œuvre de tout plan relatif à celle-ci, et accompagner les organismes publics dans cette mise en œuvre;
— coordonner les efforts des organismes publics et les soutenir dans l'adoption de pratiques de gestion optimales en matière de ressources informationnelles;
— s'assurer que les organismes publics mettent en place les meilleures pratiques en matière de cybersécurité;
— assurer une coordination gouvernementale en matière de sécurité de l'information et établir des cibles applicables à l'ensemble des organismes publics afin de mesurer leur performance sur les plans stratégique, tactique et opérationnel ainsi que l'efficacité gouvernementale dans la prise en charge des menaces, des vulnérabilités et des incidents en telle matière;
— établir des exigences en matière de sécurité de l'information applicables aux organismes publics et ordonner à ces derniers, lorsque requis, de mettre en œuvre ces exigences afin d'assurer la protection de leurs actifs informationnels et des informations qu'ils supportent;
— établir le cadre de gouvernance des projets en ressources informationnelles d'intérêt gouvernemental et assurer le développement des solutions technologiques qui y sont liées.

En matière d'infrastructures technologiques et de systèmes de soutien communs, le ministre fournirait des services aux organismes publics afin de favoriser leur transformation numérique. Cette offre serait déterminée par écrit et publiée sur le site Internet de son

ministère. Il concentrerait et développerait une expertise interne en infrastructures technologiques communes, contribuant ainsi à rehausser la sécurité de l'information numérique au sein des organismes publics et la disponibilité des services aux citoyens et aux entreprises par l'utilisation accrue d'infrastructures technologiques partagées sécuritaires et performantes. En ce sens, il devrait plus particulièrement :

- assurer l'accessibilité des services en infrastructures technologiques et en systèmes de soutien communs sous sa responsabilité;
- assurer l'adéquation de ses services avec les besoins des organismes publics, en tenant compte des priorités gouvernementales ainsi que du portefeuille des projets prioritaires, et assurer l'évolution de ces services;
- viser à optimiser les coûts de conception, de réalisation, d'exploitation et d'évolution de ses services, en vue d'améliorer l'efficience et l'efficacité de ceux-ci en fonction des objectifs de performance et de contribuer à des économies à l'échelle gouvernementale;
- mettre en place des processus de gestion de la relation avec la clientèle pour soutenir les organismes publics utilisant ses services et mesurer leur satisfaction à l'égard des services qu'il fournit;
- veiller au respect et au maintien des normes propres à assurer la confidentialité, l'intégrité et la disponibilité de l'information des organismes publics qu'il détient notamment par la mise en place de mesures de sécurité;
- contribuer à l'émergence de pratiques de gestion des technologies exemplaires et innovantes en collaboration avec les différents acteurs de l'écosystème des technologies de l'information.

Le ministre agirait également à titre de courtier infonuagique pour le compte des organismes publics, en rendant disponibles des offres infonuagiques par type de biens ou par type de services.

Le ministre pourrait fournir certains services à toute autre personne ou à toute autre entité désignée par le gouvernement.

Le ministre pourrait conclure des ententes tout comme il pourrait réaliser ou faire réaliser des consultations, des recherches, des études ou des analyses ou accorder une aide financière ou technique.

Il pourrait, s'il le juge opportun, constituer un comité qui le conseillerait dans les domaines de la cybersécurité et du numérique.

Il déterminerait la tarification ainsi que les autres formes de rémunération payables pour la prestation des services qu'il fournit, lesquels pourraient varier selon le service fourni ou la clientèle desservie. Ils seraient soumis à l'approbation du Conseil du trésor. Par la suite, la grille tarifaire devrait être publiée sur le site Internet de son ministère.

Fonds de la cybersécurité et du numérique

Le Fonds de la cybersécurité et du numérique serait créé. Il serait affecté au financement des infrastructures technologiques et des systèmes de soutien communs des organismes publics, de même que des services offerts ou fournis par le ministre, des projets ou des activités dans le domaine de la cybersécurité ou dans celui du numérique ainsi que du versement de toute aide financière accordée en vertu de ce projet de loi.

Loi concernant le cadre juridique des technologiques de l'information

Le projet de loi propose de revoir les dispositions de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1) afin de bonifier celles relatives au comité pour l'harmonisation des systèmes et des normes (articles 63 à 68) et de rendre ce comité actif.

Les changements les plus significatifs sont les suivants : i) les membres du comité seraient nommés par le ministre de la Cybersécurité et du Numérique, ii) le dirigeant principal de l'information présiderait ce comité, iii) un employé du ministère de la Justice que désigne le ministre de la Justice, membre du Barreau du Québec ou de la Chambre des notaires du Québec, siègerait à ce comité, iv) le comité pourrait formuler des recommandations quant à l'application de la loi et réaliser tout autre mandat que lui confierait le gouvernement ou le ministre de la Cybersécurité et du Numérique, v) le comité changerait de nom et deviendrait le comité pour l'harmonisation des normes, des standards et autres éléments visant l'utilisation des technologies et, finalement, vi) la responsabilité de cette loi serait confiée au ministre de la Cybersécurité et du Numérique, sauf les articles 5 à 16, 22, 27, 31, 33, 36, 37, 39, 61 et 62.

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement

Le projet de loi prévoit que le sous-ministre du ministère de la Cybersécurité et du Numérique agirait à titre de dirigeant principal de l'information. Il prévoit aussi que plusieurs responsabilités qui sont actuellement attribuées au Conseil du trésor ou au président du Conseil du trésor soient sous celle du ministre de ce nouveau ministère ou au gouvernement.

Autres dispositions

Le ministre serait substitué à ITQ eu égard à ses droits et obligations. Il serait également substitué au président du Conseil du trésor à l'égard des fonctions qui lui sont confiées par le projet de loi.

Les employés d'ITQ deviendraient des employés du ministère de la Cybersécurité et du Numérique, sauf ceux qui exercent leurs fonctions à la direction des communications, qui deviendraient des employés du ministère du Conseil exécutif, et ceux qui appartiennent à la classe d'emploi des avocats et notaires au sein de la direction des affaires juridiques d'Infrastructures technologiques Québec ou qui appartiennent à la classe d'emploi de cadre juridique de cette même direction, qui deviendraient des employés du ministère de la Justice.

Les employés du SCT affectés à des fonctions liées à celles qui seraient confiées au ministre par le projet de loi, identifiés par le président du Conseil du trésor, deviendraient également des employés du ministère de la Cybersécurité et du Numérique.

5- Autres options

Ce projet de loi est la suite logique aux modifications proposées au cadre légal en matière de ressources informationnelles depuis 2019. Il met en place la structure organisationnelle nécessaire pour concrétiser les objectifs du gouvernement en matière de transformation numérique et de cybersécurité.

Le statu quo, soit de séparer les fonctions de politiques, d'orientations, de conception, de réalisation et d'exploitation des solutions au sein de deux organisations, n'a pas été retenu, notamment en raison de la nécessité d'optimiser la gestion des projets majeurs en ressources informationnelles, de joindre les expertises en matière de cybersécurité et de transformation numérique compte tenu de la rareté de la main-d'œuvre spécialisée et de démontrer l'importance de ces sujets pour le gouvernement et pour la société civile.

6- Évaluation intégrée des incidences

La gouvernance des ressources informationnelles a été ciblée depuis quelques années pour concourir à la transformation numérique de l'État et pour continuer à protéger la sécurité des informations qu'il détient.

En instaurant une collaboration formelle avec l'écosystème du numérique, qui comprend tant le secteur public que privé, la proposition vise un accroissement de l'efficacité de la lutte contre les cyberattaques et les cybermenaces sur tout le territoire québécois.

Aucune incidence particulière négative n'est envisagée étant donné la continuité de l'offre de services d'ITQ et des fonctions du DPI au sein du nouveau ministère. L'ensemble des employés transférés conserverait leurs conditions d'emploi.

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

Le présent projet de loi n'a pas fait l'objet de consultations.

8- Mise en œuvre, suivi et évaluation

Au regard de sa mise en œuvre, une structure de projet a été mise en place pour assurer la mise en marche du nouveau ministère. Des biens livrables, ainsi que les processus liés, sont prévus sous les thèmes suivants : documents officiels, nominations, gouvernance, administration (ressources financières, ressources humaines, gestion contractuelle, ressources informationnelles), communications et gestion du changement.

Une priorisation des différents livrables permet de les séquencer pour une mise en place rapide de la nouvelle structure.

Le DPI et ITQ sont présentement deux organisations fonctionnelles, qui comportent à elles deux l'ensemble des fonctions nécessaires au bon fonctionnement de l'organisation, ce qui implique qu'aucun effectif additionnel aux postes déjà autorisés dans les deux organisations ne sera nécessaire.

En ce qui a trait à l'évaluation de la mise en œuvre de ce projet de loi, la Loi sur les ressources informationnelles prévoit déjà un rapport quinquennal portant sur les responsabilités en matière de gouvernance des ressources informationnelles.

Par ailleurs, la mise en œuvre des modifications proposées implique des ajustements aux façons de faire des organismes publics et du SCT. Les travaux requis, le cas échéant, n'impliqueront pas de financement additionnel associé à la mise en place de la structure administrative du nouveau ministère.

9- Implications financières

Les budgets actuels concernés au portefeuille Conseil du trésor et administration gouvernementale et ceux d'ITQ seront affectés à ce nouveau ministère, tout comme ceux prévus au cadre financier des années ultérieures. Cette réorganisation budgétaire fait en sorte qu'aucun impact budgétaire n'en découlera. Cette affirmation est également vraie pour le nombre d'heures rémunérées allouées ainsi que pour le budget de rémunération. En fait les modifications proposées ne nécessitent pas la création de nouveaux postes ou l'ajout d'effectifs. Ces fonctions et responsabilités seront assumées par le personnel déjà en place dans les deux organisations.

Les travaux en cours qui concernent le financement d'ITQ et de son offre de services obligatoires se poursuivront.

10- Analyse comparative

Au gouvernement du Canada, l'autorité en matière de cybersécurité est le Centre canadien pour la cybersécurité, qui regroupe les expertises de Sécurité publique du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications.

En Ontario, le Centre d'excellence en cybersécurité relève du ministère des Services gouvernementaux et des Services aux consommateurs. Un autre organisme, Services numériques de l'Ontario, a pour mission d'augmenter l'efficacité des services gouvernementaux offerts à la population à l'ère du numérique.

En Colombie-Britannique, la Dirigeante principale de l'information gère le programme d'investissements en technologies, assure la sécurité de l'information, soutient les objectifs du gouvernement en vue d'améliorer les opérations et les services au moyen des technologies de l'information et produit des stratégies, des politiques, des standards et des services technologiques pour soutenir la transformation organisationnelle du gouvernement.

En France, la Direction interministérielle du numérique (DINUM) accompagne les ministères dans leur transformation numérique, conseille le gouvernement et développe des services et ressources partagées comme le réseau interministériel de l'État, FranceConnect, data.gouv.fr ou api.gouv.fr. Elle pilote, avec l'appui des ministères, le programme TECH.GOUV d'accélération de la transformation numérique du service public.

Dans le cadre du plan France Relance, elle met en œuvre le volet Transformation numérique de l'État et des territoires, pour le compte du ministère de la Transformation et de la Fonction publiques. La DINUM est un service du Premier ministre, placé sous l'autorité de la ministre de la Transformation et de la Fonction publiques.

La France possède également, depuis juillet 2009 une Agence nationale de la sécurité des systèmes d'information (ANSSI), laquelle est rattachée au secrétaire général de la défense et de la sécurité nationale. Ce dernier assiste le Premier ministre dans l'exercice de ses responsabilités en ces matières. L'ANSSI a coordonné les travaux ministériels ayant menés au dévoilement en octobre 2015 de la Stratégie nationale pour la sécurité numérique laquelle est destinée à accompagner la transition numérique de la société française.

La France dispose aussi d'un réseau de CERT, organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT (Computer Emergency Response Team) sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, mais dont les informations sont généralement accessibles à tous.

Pour sa part, l'Allemagne peut compter sur les services du Bundesamt für Sicherheit in der Informationstechnik (BSI) [l'Office fédéral de la sécurité des technologies de l'information], une administration créée en 1991 et chargée de la sécurité des technologies de l'information et de la communication. Il s'occupe notamment de la sécurité des logiciels, de la protection des infrastructures de communications, de la sécurité dans le cyberespace, de cryptographie, de contre-écoute électronique, de certification de produits de sécurité et de l'accréditation de laboratoires de test.

C’est une administration fédérale supérieure placée sous la tutelle du ministère fédéral de l’Intérieur.

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