

DE : Monsieur Éric Caire
Ministre de la Cybersécurité et du Numérique

Le 3 juillet 2024

TITRE : Stratégie gouvernementale de cybersécurité et du numérique 2024-2028

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

En 2019, le gouvernement du Québec a adopté la Stratégie de transformation numérique gouvernementale 2019-2023 (ci-après « Stratégie 2019-2023 ») dans le but de fournir à l'administration publique une vision commune et cohérente en vue de réaliser la transformation de l'État par le numérique. Cette vision était claire : des services publics plus rapides et intuitifs, propulsés par le numérique.

La Stratégie 2019-2023 a eu pour effet d'engager l'administration publique sur la voie de la transformation numérique en fournissant des structures de gouvernance en ressources informationnelles solides, permettant une action concertée et structurante entre les organismes publics. Ainsi, depuis 2019, le gouvernement du Québec se démarque par ses réalisations en matière de transformation numérique de l'administration publique et de cybersécurité.

Les technologies du numérique sont au cœur du contexte stratégique dans lequel évoluent les organismes publics. Ce dernier a grandement évolué au cours des quatre dernières années durant lesquelles s'est réalisée la Stratégie 2019-2023. À ce chapitre, pensons notamment aux éléments suivants :

- l'accélération sans précédent des développements technologiques, notamment ceux résultants de l'utilisation de l'intelligence artificielle;
- le nombre croissant des cyberattaques dans le monde et au Québec, menaçant les citoyens, les entreprises et les administrations publiques;
- le recours accru à l'infonuagique, qui a un impact important sur les organisations quant au développement et à la gestion de leurs services numériques;
- la rareté de main-d'œuvre, incluant celle spécialisée en ressources informationnelles, qui menace désormais la capacité de maintien et d'évolution des services publics;
- la croissance rapide de l'utilisation du numérique et de l'appétit pour les services numériques au sein de la population, de même que le télétravail;
- le caractère de plus en plus crucial que représentent les données pour les organisations; la protection et la valorisation de ces dernières s'imposant maintenant comme un levier essentiel de compétitivité.

Il devient ainsi indispensable pour le gouvernement du Québec d'adapter sa stratégie en matière de cybersécurité et du numérique laquelle doit s'adapter à cet environnement en perpétuelle évolution.

En vertu de l'article 2 de la Loi sur le ministère de la Cybersécurité et du Numérique (chapitre M-17.1.1), le ministre de la Cybersécurité et du Numérique doit établir des objectifs et élaborer des politiques, des stratégies et des programmes propres à assurer l'accomplissement de sa mission, laquelle consiste à animer et coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique. C'est dans ce cadre que s'inscrit la proposition de la présente stratégie.

À des fins de cohérence, la *Politique gouvernementale de cybersécurité*, en vigueur depuis 2020, et la *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021-2026* seront désormais associées à la Stratégie 2024-2028.

2- Raison d'être de l'intervention

Le numérique occupe une place centrale dans la vie d'une grande majorité de Québécoises et de Québécois. En 2022, au Québec¹ :

- 95 % des adultes québécois possèdent un appareil électronique. Cette proportion passe à 100 % pour les 25 à 44 ans et est de 79 % pour les 75 ans et plus.
- 84 % des citoyens sont propriétaires d'un téléphone intelligent, alors que ce taux était de 77 % en 2019.
- Le téléphone intelligent est le principal appareil utilisé pour naviguer sur Internet.

Cette omniprésence du numérique de même que la multiplication des plateformes technologiques de haute qualité offertes par un nombre croissant d'organisations du secteur privé fait en sorte que les citoyennes et les citoyens² s'attendent désormais aux plus hauts standards en matière de services numériques de la part de l'administration publique.

Malgré les avancées réalisées dans le cadre de la Stratégie 2019-2023, l'administration publique rencontre encore de nombreux défis dans plusieurs domaines d'actions liés à la cybersécurité et au numérique.

En matière de transformation des services publics

Le numérique est omniprésent dans le quotidien des citoyennes et des citoyens. La population a des attentes élevées en matière d'accès et d'utilisation des services en ligne, notamment par son expérience lors de l'utilisation de ceux offerts par le secteur privé. De ce fait, l'administration publique doit s'adapter aux nouveaux standards en rendant ses services plus simples, rapides, personnalisés et requérant moins d'interactions. L'État doit également unifier ses services pour que les citoyennes et les citoyens aient l'impression

¹ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE. (2022). *Portrait numérique des foyers québécois. Édition 2022*, [En ligne], [<https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/portrait-numerique-des-foyers-quebecois-2022/>], (Consulté en avril 2023).

² Le terme « citoyen » inclut les entreprises (citoyens corporatifs) lorsque cela est applicable.

d'interagir avec une seule et même organisation lorsqu'ils échangent avec différents organismes publics. De surcroît, l'État doit veiller à éviter la fracture numérique, en s'assurant que ses services soient accessibles pour toutes et tous peu importe leur situation socio-économique, géographique ou leur niveau de littératie numérique.

En matière de protection des données

Pour veiller à ce que le public conserve sa confiance envers l'administration publique quant à la protection de ses renseignements personnels, celle-ci doit maintenir sa capacité à protéger de tels renseignements et les nombreuses données sous sa responsabilité. Dès lors, l'administration publique doit non seulement continuer à développer et utiliser des outils de sécurité innovants, mais aussi s'assurer que son personnel ait les compétences et les réflexes nécessaires en matière de cybersécurité.

En matière de valorisation des données

L'administration publique détient une quantité importante de données présentant un haut potentiel de valorisation. En utilisant celles-ci de façon éthique et responsable, les organismes publics ont l'occasion d'améliorer de façon significative la prestation de services à la population, notamment en évitant de demander plusieurs fois les mêmes informations dans ses différentes interactions avec les citoyennes et citoyens. À cet effet, une approche collaborative entre les organismes publics doit être adoptée. De plus, en démocratisant l'accès aux données et en encourageant l'innovation en cette matière, l'État peut contribuer à renforcer la confiance du public, à stimuler la croissance économique et à améliorer la qualité de vie des citoyennes et citoyens.

En matière d'intelligence artificielle

L'intelligence artificielle a fait l'objet de développements significatifs au cours des dernières années, façonnant l'ensemble des secteurs d'activités et s'imposant désormais comme un sujet incontournable. L'intelligence artificielle et l'automatisation présentent un potentiel important pour accroître la performance et l'excellence opérationnelle de l'administration publique ainsi que la qualité des services offerts aux citoyennes et citoyens. Toutefois, le développement de l'intelligence artificielle, dans l'administration publique comme dans la société civile, nécessite un cadre qui tout en permettant d'en retirer les bienfaits s'assurera de limiter les biais et les dérives potentielles.

En matière de sécurité de l'information

Le contexte technologique étant en constante évolution, il est nécessaire de veiller perpétuellement à l'adéquation du niveau de maturité des organismes publics avec celui-ci. L'administration publique doit adapter sa pratique aux nouvelles menaces afin d'établir une posture de sécurité³, lui permettant de faire face à celles-ci, notamment en misant sur un réseau de cyberdéfense où les organismes publics mettent en commun leurs efforts et leurs expertises.

³ Un état dans lequel un organisme, un individu se sent en sécurité.

En matière de gestion des ressources informationnelles

Le contexte de rareté des ressources, qu'elles soient humaines, financières ou matérielles, ne permet pas de réaliser toutes les initiatives de transformation numérique dans les délais souhaités. L'administration publique doit donc veiller à ce que les projets qui sont priorisés soient ceux qui engendrent le plus de bénéfices et qui sont alignés avec les priorités gouvernementales. Plus que la gestion des projets et la priorisation, l'État doit veiller à ce que l'acquisition en compétences et en expertises soit constamment au diapason de l'évolution des technologies, notamment dans les secteurs critiques de la cybersécurité et de l'intelligence artificielle.

En matière de mutualisation

Toujours dans ce contexte de rareté des ressources, la mutualisation des services, des infrastructures, de l'expertise et des ressources s'avère un outil incontournable pour mener la transformation numérique en optimisant les ressources disponibles. L'administration publique doit mettre en place un véritable cadre permettant aux organismes publics de partager différents services ou d'utiliser des fondations numériques communes.

En matière d'infrastructures technologiques

L'administration publique possède une quantité importante de données. Celle-ci doit s'assurer que cette information est stockée de façon sécuritaire et performante. En ce sens, la migration de l'information vers l'infonuagique gouvernementale ainsi que vers un nombre optimal de centres de traitement informatique est essentielle.

En matière gestion des actifs informationnels

Le niveau de désuétude de certains actifs informationnels et solutions d'affaires rend parfois difficile l'interopérabilité de ces solutions et de ces actifs avec d'autres, qui sont plus récents. Cette situation, en plus de freiner l'amélioration des services numériques offerts aux citoyennes et aux citoyens, peut constituer un risque en continuité des opérations et plus globalement en sécurité de l'information. Dans les prochaines années, l'administration publique devra mettre en œuvre des stratégies pour résorber cette désuétude.

En matière d'infrastructures de connectivité

Pour veiller au bon déroulement de la transformation numérique, mais également au développement économique et social du Québec, ce dernier doit pouvoir s'appuyer sur un réseau d'infrastructures de connectivité et de télécommunications de pointe. Ceci représente non seulement un enjeu de productivité et d'efficacité, mais également de cybersécurité.

3- Objectifs poursuivis

La Stratégie 2024-2028 s'inscrit en continuité avec la Stratégie 2019-2023. Elle ne cherche pas à rompre avec les orientations qui y étaient énoncées. Elle est une réponse aux nouveaux enjeux auxquels fait face l'administration publique en matière de cybersécurité et du numérique.

Elle vise à poursuivre la propulsion de l'administration publique à l'ère du numérique en proposant une vision commune renouvelée de l'action de l'État dans les domaines de la cybersécurité et du numérique. Elle a aussi pour objectif d'inspirer la confiance des citoyennes et des citoyens dans la capacité de l'administration publique québécoise à réaliser des projets porteurs de transformation par le numérique lesquels contribueront significativement à améliorer la qualité des services et à simplifier leur vie quotidienne.

4- Proposition

La Stratégie 2024-2028 s'applique à l'ensemble des organismes publics assujettis 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 « Loi sur les ressources informationnelles »), ce qui représente un peu plus de 300 organismes publics, dont ceux des réseaux de l'éducation, de l'enseignement supérieur et de la santé et des services sociaux.

La Stratégie 2024–2028 s'articule en trois axes, lesquels regroupent 10 objectifs.

Axe 1 : Accroître la cybersécurité de l'administration publique

La transformation numérique de l'administration publique nécessite que la gestion des risques en sécurité de l'information soit prise en compte dès le départ afin d'éviter la perturbation ou l'arrêt des services essentiels à la population, ou encore le vol de données. Ces défis mettent en lumière la nécessité d'assurer la protection des données des citoyennes et citoyens ainsi que celles des organisations à l'égard des cybermenaces ainsi que la résilience des services publics et des infrastructures critiques. Ainsi, la cybersécurité s'impose comme un pilier essentiel de l'évolution de la société à l'ère du numérique.

Dans ce contexte, l'État doit être exemplaire et s'imposer comme un chef de file en veillant à ce que sa propre transformation numérique soit réalisée dans un environnement cybersécuritaire. L'exemplarité de l'administration publique en cette matière revêt une importance particulière, car elle constitue un facteur clé pour développer et maintenir la confiance des citoyennes et des citoyens à l'égard de sa capacité à prévenir les incidents de sécurité, à assurer la résilience de ses services offerts à la population et à conduire une transformation numérique réussie.

L'État entend ainsi renforcer la sécurité de l'information, des services publics notamment en augmentant sa capacité à cibler les menaces, les vulnérabilités et à prévenir les incidents de cybersécurité tout comme il s'engage à protéger les données des citoyennes, des citoyens et des entreprises et de l'administration publique.

Axe 2 : Accélérer la transformation numérique de l'administration publique

Cet axe vise à poursuivre et accélérer la transformation numérique de l'administration publique qui a été entamée dans le cadre de la mise en œuvre de la Stratégie 2019-2023.

Cette transformation en profondeur amène l'administration publique à devoir réinventer plusieurs aspects de son organisation, soit la manière dont elle conçoit et rend les services à la population, la manière dont elle gère ses données et conçoit ses processus d'affaires pour générer de la valeur et sa manière d'aborder le changement et de stimuler l'innovation. Ces changements de paradigme sont incontournables.

Ainsi, il est proposé d'une part qu'une offre unifiée de services numériques gouvernementaux soit instaurée et d'autre part, que des travaux visant à accroître la mobilité et la valorisation des données numériques gouvernementales soient menés.

Également, l'intelligence artificielle sera mise à profit afin d'accroître la performance de l'administration publique.

Finalement, les projets en ressources informationnelles feront l'objet d'une attention particulière afin d'en assurer le succès tout comme la mutualisation de fondations numériques gouvernementales sera encouragée.

Axe 3 : Développer des infrastructures technologiques pérennes et sécuritaires

Les infrastructures technologiques et les actifs informationnels jouent un rôle essentiel dans le déploiement de la transformation numérique pour l'administration publique, mais également pour la cybersécurité. Ce sont eux qui rendent possible cette transformation.

Les infrastructures technologiques assurent notamment la connectivité nécessaire au fonctionnement des technologies numériques, la sécurité et la circulation des données, en plus de permettre le stockage sécuritaire de ces dernières. Elles constituent les fondations qui permettent de développer des services numériques qu'ils soient en lien avec la mission d'une organisation ou en soutien à celle-ci. Des infrastructures à jour permettent à l'État de se transformer et d'évoluer en tenant compte des exigences qui sont notamment tributaires à des enjeux de sécurité.

Les actifs informationnels de l'administration publique, quant à eux, sont les fondations qui permettent à ses programmes et services de fonctionner. Il importe de s'assurer que ceux-ci continuent de répondre aux besoins et qu'ils évoluent de manière à ne pas poser de risque pour la sécurité de l'information ou à la continuité des services.

Dans cette perspective, des actions seront prises afin d'accélérer le passage à l'infonuagique, de résorber la désuétude des actifs informationnels ainsi que pour déployer des infrastructures de connectivité et de télécommunication, le tout afin de garantir la pérennité et la sécurité numérique de l'administration publique.

Tableau 1

Sommaire des axes, des objectifs et des cibles de la Stratégie 2024-2028

Axes	Objectifs	Indicateurs	Période	Cibles
1. Accroître la cybersécurité de l'administration publique	1. Renforcer la sécurité de l'information des services publics	Pourcentage de centres opérationnels de cyberdéfense intégrés dans le service de détection et de surveillance des événements de sécurité offerts par le Centre gouvernemental de cyberdéfense	2024-2025	10 %
			2025-2026	20 %
			2026-2027	45 %
			2027-2028	70 %
	2. Protéger les données des citoyennes et des citoyens, des entreprises et de l'administration publique	Pourcentage des organismes publics ayant commencé l'application du marquage des données non structurées prévu au modèle de classification de sécurité des données numériques gouvernementales	2024-2025	10 %
			2025-2026	40 %
			2026-2027	80 %
			2027-2028	100 %
2. Accélérer la transformation numérique de l'administration publique	3. Instaurer une offre unifiée de services numériques gouvernementaux	Pourcentage des prestations électroniques de services (PES) des organismes publics, s'adressant aux citoyennes et aux citoyens, arrimées au Service d'authentification gouvernementale	2024-2025	8 %
			2025-2026	23 %
			2026-2027	48 %
			2027-2028	100 %
	4. Accroître la mobilité et la valorisation des données numériques gouvernementales	Pourcentage d'organismes publics ayant commencé la démarche de cartographie et d'inventaire des données numériques gouvernementales	2024-2025	15 %
			2025-2026	30 %
			2026-2027	60 %
			2027-2028	100 %
		Pourcentage de sources officielles de données identifiées et exploitables	2024-2025	Détermination des sources officielles de données prioritaires exploitables
			2025-2026	15 %
			2026-2027	30 %
			2027-2028	50 %

Axes	Objectifs	Indicateurs	Période	Cibles
	5. Accroître la performance de l'administration publique grâce à l'intelligence artificielle responsable	Augmentation du nombre d'initiatives en intelligence artificielle dans l'administration publique	2024-2025	Prise de la mesure
			2025-2026	Augmentation de 10 %
			2026-2027	Augmentation de 10 %
			2027-2028	Augmentation de 10 %
	6. Maximiser les retombées des projets en ressources informationnelles et en assurer le succès	Somme des bénéfices quantifiables et récurrents identifiés dans les plans de matérialisation des bénéfices des projets qualifiés des organismes publics ainsi que des économies récurrentes générées dans le cadre de l'offre de service du ministère de la Cybersécurité et du Numérique	2024-2025	100 M\$
			2025-2026	150 M\$
			2026-2027	200 M\$
			2027-2028	200 M\$
	7. Favoriser la mutualisation et la mise en œuvre de fondations numériques gouvernementales	Pourcentage des nouveaux projets qualifiés en ressources informationnelles ayant fait l'objet d'une analyse sur la possibilité de mutualiser ou de réutiliser des solutions existantes entre les organismes publics au cours de la phase de planification	2024-2025	70 %
			2025-2026	80 %
			2026-2027	80 %
			2027-2028	80 %
3. Développer des infrastructures technologiques pérennes et sécuritaires	8. Consolider les actifs technologiques	Pourcentage d'organismes publics dont la stratégie respecte l'orientation gouvernementale de consolidation des centres de traitement informatique	2024-2025	75 %
			2025-2026	95 %
			2026-2027	100 %
			2027-2028	S. O.
	9. Résorber la désuétude des actifs informationnels de l'administration publique	Pourcentage des actifs informationnels en voie d'être désuets ou désuets faisant l'objet d'une stratégie d'intervention	2024-2025	S. O. (Collecte tous les 2 ans)
			2025-2026	75 %
			2026-2027	S. O. (Collecte tous les 2 ans)
			2027-2028	90 %

Axes	Objectifs	Indicateurs	Période	Cibles
	10. Soutenir le déploiement des infrastructures de télécommunication	Pourcentage des services du Réseau intégré de télécommunication multimédia (RITM) ayant migré vers le Réseau gouvernemental de télécommunication (RGT)	2024-2025	25 %
			2025-2026	65 %
			2026-2027	85 %
			2027-2028	100 %

5- Autres options

Il a été envisagé d'adopter une stratégie en matière de cybersécurité et du numérique qui aurait eu une portée plus large que l'administration publique et qui aurait notamment visée à structurer l'action gouvernementale dans des domaines autant auprès de la société civile que du secteur public.

Une telle stratégie aurait notamment abordé des enjeux tels que le soutien à la recherche en matière de cybersécurité et du numérique, la régulation de l'utilisation du numérique par les entreprises et le gouvernement, le développement des infrastructures technologiques sur le territoire, etc.

Cette option n'a toutefois pas été retenue, puisqu'il a été considéré que la cybersécurité et le numérique dans l'administration publique représentent des défis suffisamment importants pour justifier leur propre stratégie.

6- Évaluation intégrée des incidences

Citoyens

En plaçant les besoins des utilisateurs au centre de la conception et de l'évolution des services numériques, en plus de viser des services plus simples, unifiés, conviviaux et sécuritaires, la Stratégie 2024-2028 aura une incidence directe et positive sur la qualité des services publics offerts aux citoyennes et aux citoyens ainsi qu'aux entreprises du Québec.

De plus, en visant à instaurer une offre unifiée de services gouvernementaux, la Stratégie 2024-2028 aura un impact direct sur l'expérience des citoyennes et des citoyens à l'égard du gouvernement en faisant en sorte qu'ils n'aient pas l'impression de faire affaire avec plusieurs entités lorsqu'ils utilisent des services numériques, mais bien avec un seul gouvernement.

Dans la même lignée, la Stratégie 2024-2028 vise à stimuler l'innovation, l'automatisation et la transformation en profondeur des processus au sein des organismes publics dans un objectif d'accroître la productivité de l'administration publique grâce au numérique et ainsi maximiser les bénéfices de la transformation numérique pour les citoyennes et les citoyens.

Également, la Stratégie 2024-2028 accorde une attention particulière aux enjeux liés à la fracture numérique⁴ et à la prise en compte des différentes réalités des citoyennes et des citoyens dans la conception des services, ce qui favorisera des services accessibles et adaptés aux réalités de tous les groupes de la population.

Dimension sociale

La mise en œuvre de la Stratégie 2024-2028 devrait avoir une incidence directe sur la lutte aux inégalités sociales en positionnant la fracture numérique comme un enjeu majeur auquel les organismes publics doivent porter une attention particulière dans le développement de leurs services numériques afin d'en minimiser les impacts.

Ainsi, dans le cadre de la Stratégie 2024-2028, le gouvernement s'engage à fournir des services numériques de qualité à toute la population, sans égard à l'origine, au genre, à l'âge, à la situation géographique ou à toute autre condition socio-économique, tout en respectant les besoins de toute la population du Québec et en continuant d'offrir des services en mode traditionnel aux personnes qui en font la demande.

Également, dans une optique d'équité intergénérationnelle, la Stratégie 2024-2028 a comme vision d'assurer des services publics durables, résilients et résolument tournés vers l'avenir pour les générations futures.

Dimension environnementale et territoriale

La Stratégie 2024-2028 devrait contribuer à améliorer l'efficacité énergétique des infrastructures technologiques de l'administration publique en favorisant la mutualisation et la réutilisation des solutions technologiques entre les organismes publics ainsi que la numérisation des services et, par conséquent, la dématérialisation de ces derniers, notamment par le biais de l'infonuagique.

De plus, consciente de l'impact du numérique sur la croissance des émissions de gaz à effet de serre, la Stratégie 2024-2028 vise à s'assurer que le développement des technologies de l'information au sein de l'administration publique se fasse en respect des principes de développement durable.

Par ailleurs, la Stratégie 2024-2028 n'a pas d'incidence directe sur les territoires, les régions, la Capitale-Nationale et la métropole. Cela dit, la transformation numérique des services de l'administration publique entraînera inévitablement une meilleure accessibilité aux services publics pour les personnes habitant en région éloignée.

Dimension économique

La Stratégie 2024-2028 devrait avoir une incidence indirecte sur le marché de l'emploi en favorisant le recrutement, au sein de l'administration publique, de spécialistes liés aux domaines de la cybersécurité et du numérique.

⁴ Le concept de fracture numérique fait référence aux inégalités entre les individus, les communautés et les pays en termes d'accès à l'information et aux technologies numériques.

Dimension gouvernance

En faisant de la diffusion d'un plus grand nombre de données ouvertes et de l'amélioration de l'accès à l'information une priorité stratégique, la Stratégie 2024-2028 aura un impact direct et positif sur la transparence de l'administration publique.

En ce qui concerne les relations avec les gouvernements fédéral, provinciaux et territoriaux, l'adoption de la Stratégie 2024-2028 pourrait contribuer à développer certaines avenues de collaboration, puisque la cybersécurité et le numérique sont des questions communes à tous les gouvernements. À ce chapitre, la Stratégie 2024-2028 place la collaboration avec l'écosystème de cybersécurité et du numérique au centre de son opérationnalisation, ce qui implique également des impacts indirects sur les relations internationales en raison de potentielles collaborations avec d'autres gouvernements à l'échelle internationale.

Finalement, puisque la Stratégie 2024-2028 vise à offrir une vision commune à l'administration publique en matière de cybersécurité et du numérique ainsi qu'à assurer de l'action concertée entre les organismes publics, elle aura un impact direct sur les responsabilités administratives de ces derniers.

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

L'élaboration de la Stratégie 2024-2028 a été facilitée par des consultations réalisées auprès des membres du Comité de gouvernance en ressources informationnelles, lequel est présidé par le dirigeant principal de l'information et réunit tous les dirigeants de l'information⁵.

Ces travaux ont permis aux membres du Comité de gouvernance en ressources informationnelles d'exprimer leurs besoins, leurs commentaires et leurs suggestions à l'égard de la vision, des axes, des objectifs et des priorités stratégiques qui devraient composer la Stratégie 2024-2028.

Par ailleurs, le ministère de la Cybersécurité et du Numérique a pu s'appuyer sur le Comité d'experts en matière de cybersécurité et du numérique, constitué par le ministre de la Cybersécurité et du Numérique en vertu de la Loi sur le ministère de la Cybersécurité et du Numérique, lesquels ont identifié les priorités d'action ainsi que les grandes orientations à aborder dans la Stratégie 2024-2028.

En soutien à l'élaboration de la Stratégie 2024-2028, des travaux ont été menés par la Chaire de recherche en exploitation des ressources informationnelles de l'École nationale d'administration publique. Ces travaux ont mené à la production d'un rapport intitulé « La gouvernance informationnelle comme levier à la transformation vers le numérique : état des

⁵ Des dirigeants de l'information sont présents dans les ministères ou organismes suivants : Affaires municipales et Habitation; Agriculture, Pêcheries et Alimentation; Conseil du trésor et Administration gouvernementale; Conseil exécutif; Culture et Communications; Cybersécurité et Numérique; Économie, Innovation et Énergie; Éducation; Emploi et Solidarité sociale; Enseignement supérieur; Environnement, Lutte contre les changements climatiques, Faune et Parcs; Famille; Finances; Immigration, Francisation et Intégration; Justice; Langue française; Relations internationales et Francophonie; Ressources naturelles et Forêts; Santé et Services sociaux; Sécurité publique; Tourisme; Transports et Mobilité durable; Travail; Commission des normes, de l'équité, de la santé et de la sécurité du travail; Régie de l'assurance maladie du Québec; Retraite Québec; Revenu Québec; Société de l'assurance automobile du Québec; Sûreté du Québec.

lieux » et ont permis d'identifier les principaux défis à aborder dans la Stratégie 2024-2028 ainsi que les orientations à établir pour y répondre.

Pour certains éléments de la Stratégie 2024-2028, le Secrétariat du Conseil du trésor, le ministère de l'Emploi et de la Solidarité sociale, le Secrétariat à l'Internet haute vitesse et aux projets spéciaux de connectivité et le Secrétariat à la communication gouvernementale, tous deux du ministère du Conseil exécutif, ont formulé des commentaires qui ont été pris en compte.

8- Mise en œuvre, suivi et évaluation

Coordination à l'échelle gouvernementale

Dans un esprit de mise en œuvre concertée au sein de l'administration publique, un suivi régulier de l'avancement et de l'opérationnalisation de la Stratégie 2024-2028 sera effectué par le Comité de gouvernance en ressources informationnelles.

Contribution des organismes publics

Depuis 2021, la Loi sur les ressources informationnelles prévoit que les organismes publics ont l'obligation d'établir un plan de transformation numérique qui se veut un vecteur d'innovation pour l'amélioration des services gouvernementaux.

Lors de leur révision annuelle, les plans de transformation numérique des organismes publics devront être alignés avec la Stratégie 2024-2028 et préciser comment l'organisme prévoit contribuer à l'atteinte des cibles gouvernementales qui les concernent.

Les plans de transformation numérique permettront ainsi de structurer l'action des organismes publics en vue de concrétiser la vision gouvernementale en matière de cybersécurité et du numérique.

Suivi et reddition de comptes

Mis en ligne en 2020, le Baromètre numériQc (ci-après « le Baromètre ») est un outil simple et visuel permettant de partager publiquement les avancées de la transformation numérique de l'administration publique.

Dans la première année de la mise en œuvre de la Stratégie 2024-2028, le Baromètre évoluera pour incorporer les nouvelles cibles gouvernementales en matière de cybersécurité et du numérique.

Les résultats relatifs à l'atteinte des cibles seront publiés annuellement sur le Baromètre.

9- Implications financières

La Stratégie 2024-2028 propose une vision globale et concertée en matière de ressources informationnelles pour toute l'administration publique, qui ne se traduit généralement pas par la mise en œuvre de nouvelles actions précises par les organismes publics, lesquelles nécessiteraient des investissements supplémentaires. Plutôt, elle implique des ajustements aux façons de faire des organismes publics, qui pourront se refléter dans les actions qui seront inscrites dans leur plan de transformation numérique respectif.

Le ministère de la Cybersécurité et du Numérique mettra en place un certain nombre d'actions dans le but de favoriser l'atteinte des cibles gouvernementales par les organismes publics. Il n'est pas prévu que ces mesures aient des implications financières pour les organismes publics.

10- Analyse comparative

La Stratégie 2024-2028 a été élaborée en prenant en compte un exercice de balisage effectué auprès de plus de 15 gouvernements (Australie, Argentine, Canada, Ontario, Colombie-Britannique, Corée du Sud, Danemark, Estonie, Finlande, États-Unis, Norvège, Ontario, Royaume-Uni, Singapour, Union européenne). Par conséquent, c'est près d'une quarantaine de stratégies gouvernementales qui ont été analysées dans le cadre des présents travaux.

Ainsi, avec la Stratégie 2024-2028, le gouvernement du Québec propose une vision en adéquation avec ce que proposent plusieurs autres États qui placent la cybersécurité et le numérique comme étant des priorités gouvernementales.

Néanmoins, il importe de noter que plusieurs documents analysés proposent des stratégies gouvernementales distinctes pour aborder les questions liées à la cybersécurité et au numérique. Cela n'est pas étranger au fait que ces États ne possèdent pas de ministère ou de département traitant de ces questions de manière globale. Par exemple, les questions de cybersécurité sont régulièrement portées par l'autorité responsable de la sécurité publique alors que les questions du numérique peuvent relever d'une autre autorité responsable des questions d'économie et d'innovation.

Tableau 2

Comparatif des domaines d'action en matière de cybersécurité et du numérique abordés par les stratégies gouvernementales des principaux gouvernements observés

Domaines d'action liés aux objectifs de la Stratégie 2024-2028	Royaume-Uni	Estonie	Canada	Australie
Sécurité de l'information et cybersécurité	•	•	•	•
Citoyenneté numérique	•	•	•	•
Numérique responsable et durable	•	•		
Transformation des services	•	•	•	•

Domaines d'action liés aux objectifs de la Stratégie 2024-2028	Royaume-Uni	Estonie	Canada	Australie
Gestion des données numériques et innovation	•	•	•	•
Culture numérique	•	•	•	•
Gouvernance et financement des ressources informationnelles	•	•	•	•
Main-d'œuvre en ressources informationnelles et expérience employé	•	•	•	•
Infrastructures technologiques et désuétude	•	•	•	•

Royaume-Uni

Pour l'administration publique, le gouvernement britannique a publié la feuille de route « Transforming for a digital future : 2022 to 2025 roadmap for digital and data » en avril 2022⁶. Cette feuille de route avait pour objectif de mettre en place des services publics transformés axés sur les résultats; un seul point d'accès aux services en ligne; une meilleure gouvernance des données pour favoriser la prise de décision; l'utilisation de la technologie de façon efficiente, sécuritaire et durable; le développement de compétences numériques à jour pour toute l'administration; la révision des processus d'affaires et de gouvernance pour faciliter la transformation numérique.

En matière de cybersécurité, l'administration publique s'est aussi dotée de la Stratégie gouvernementale en cybersécurité (2022-2030)⁷. Elle vise à s'assurer que les fonctions principales de l'administration publique, de la livraison des services publics au fonctionnement de l'appareil de sécurité nationale soient résilientes face aux cyberattaques, renforçant le Royaume-Uni comme nation souveraine et appuyant sa position comme étant un « cyberpouvoir démocratique et responsable ».

Estonie

En 2022, l'Estonie s'est classée première dans le « classement global des services numériques » de l'Organisation des Nations Unies⁸. Ainsi, l'Estonie est considérée comme l'un des pays les plus avancés au monde en ce qui concerne la transformation numérique. La population peut accéder à la quasi-totalité des services gouvernementaux de façon totalement numérique, à l'exception de quelques services comme le mariage, le divorce et l'achat ou la vente d'immobilier. Elle le fait notamment via « le X-Road⁹ », un protocole de communication multicanal conçu pour la prestation de tous les services numériques, avec

⁶ GOUVERNEMENT DU ROYAUME-UNI. « Transforming for a digital future: 2022 to 2025 roadmap for digital and data », [en ligne], [\[https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data\]](https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data).

⁷ GOUVERNEMENT DU ROYAUME-UNI. « Government cyber-security strategy 2022 to 2030 », [en ligne], [\[https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html\]](https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html).

⁸ ORGANISATION DES NATIONS UNIES. « E-Government Survey 2022 », [en ligne], [\[https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf\]](https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf).

⁹ GOUVERNEMENT DE L'ESTONIE. « X-Road », [en ligne], [\[https://e-estonia.com/solutions/interoperability-services/x-road/\]](https://e-estonia.com/solutions/interoperability-services/x-road/).

des fonctions sécuritaires comme l'identité numérique, le vote en ligne, l'impôt en ligne et le commerce numérique. Par ailleurs, la plateforme Web « Esti.ee » est un guichet unique en ce qui concerne les informations sur l'administration publique et les services numériques.

Les stratégies gouvernementales de l'Estonie se tournent principalement vers la société civile, que ce soit en matière de numérique ou de cybersécurité. À cet effet, elle a publié dans les dernières années l'Agenda numérique pour l'Estonie (2030) qui vise à développer une réelle société axée sur le numérique¹⁰, ainsi que la Stratégie en cybersécurité (2019-2022) qui a pour ambition de faire de « l'Estonie la société numérique la plus résiliente¹¹ ».

Canada

En août 2022, Ambition numérique du Canada (ANC)¹² a été lancée par le Secrétariat du Conseil du Trésor du gouvernement du Canada. L'ANC 2022 vise à « faciliter la prestation de services gouvernementaux à l'ère numérique pour tous les Canadiens en fournissant des outils modernisés et accessibles pour soutenir une prestation de services qui expriment le meilleur du Canada dans l'espace numérique ».

Avec l'ANC 2022, le gouvernement du Canada souhaite offrir une vision claire et à long terme pour développer et faire évoluer la prestation de services numériques aux citoyens, la cybersécurité, le recrutement de talents et la protection de la vie privée.

Pour le gouvernement du Canada, l'ANC 2022 représente un fondement clé soutenant la transformation numérique de l'État canadien. Les ministères doivent développer leur propre plan intégré en conformité avec l'ANC 2022 en tenant compte de leur mandat et obligations.

Les priorités de l'ANC sont les suivantes :

1. l'excellence en matière de technologies et d'opérations, ce qui comprend un paysage technique sans risque et des pratiques modernes, souples et axées sur les personnes;
2. des services et des programmes numériques plus simples, fiables et étayés par l'intégration et la gestion des données à l'échelle du gouvernement;
3. des politiques et des cadres directeurs conçus pour un gouvernement numérique moderne, sûr et axé sur la protection des renseignements personnels;
4. des employés autonomisés dotés de talents numériques optimisés et perfectionnés dans l'ensemble du gouvernement du Canada, reconnaissant que les talents numériques dans l'ensemble du Canada sont très recherchés.

¹⁰ GOUVERNEMENT DE L'ESTONIE. « Estonia's Digital Agenda 2030 », [en ligne], [\[https://www.mkm.ee/media/6970/download\]](https://www.mkm.ee/media/6970/download).

¹¹ GOUVERNEMENT DE L'ESTONIE. « Cybersecurity strategy », [en ligne], [\[https://www.mkm.ee/media/703/download#:~:text=This%20cybersecurity%20strategy%20is%20Estonia's,activity%20planning%20and%20resource%20allocation%20\]](https://www.mkm.ee/media/703/download#:~:text=This%20cybersecurity%20strategy%20is%20Estonia's,activity%20planning%20and%20resource%20allocation%20).

¹² GOUVERNEMENT DU CANADA. « Ambition numérique du Canada », [en ligne], [\[https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/ambition-numerique-canada.html\]](https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/ambition-numerique-canada.html).

Australie

En 2021, l'Agence de transformation numérique de l'Australie adopte la « Stratégie du gouvernement numérique : accélération de l'avenir numérique de notre administration publique australienne (2021-2025)¹³ ». Celle-ci est composée de deux axes stratégiques :

1. L'axe « communauté et entreprises » vise l'atteinte des résultats suivants :

- Disponibilité :
Les Australiens pourront interagir avec l'administration publique à partir de n'importe où, n'importe quand et sur n'importe quel appareil.
- Facilité d'accès :
Les services seront faciles à utiliser, accessibles et connectés pour que les Australiens puissent rentrer en communication avec l'administration publique à partir d'un seul point d'entrée.
- Centré sur la communauté et les entreprises :
Les services numériques seront conçus pour l'utilisateur avec une apparence et un style uniforme et centrés autour des événements de vie.

2. L'axe « administration publique » vise l'atteinte des résultats suivants :

- Alignement de l'architecture :
Élever l'écosystème et l'ajouter aux plateformes et services connectés à l'intérieur de l'architecture numérique gouvernementale.
- Réutiliser et investir :
Une culture de réutilisation est appuyée sur des capacités modernes numériques qui optimisent les ressources via des processus d'investissements dynamiques.
- Milieu de travail numérique :
Construire une administration publique adaptée à l'ère numérique, habilitée par les compétences, capacités et outils numériques.

Le ministre de la Cybersécurité et du
Numérique,

ÉRIC CAIRE

¹³ GOUVERNEMENT DE L'AUSTRALIE. « Digital Government Strategy », [en ligne], [\[https://www.dta.gov.au/digital-government-strategy\]](https://www.dta.gov.au/digital-government-strategy).