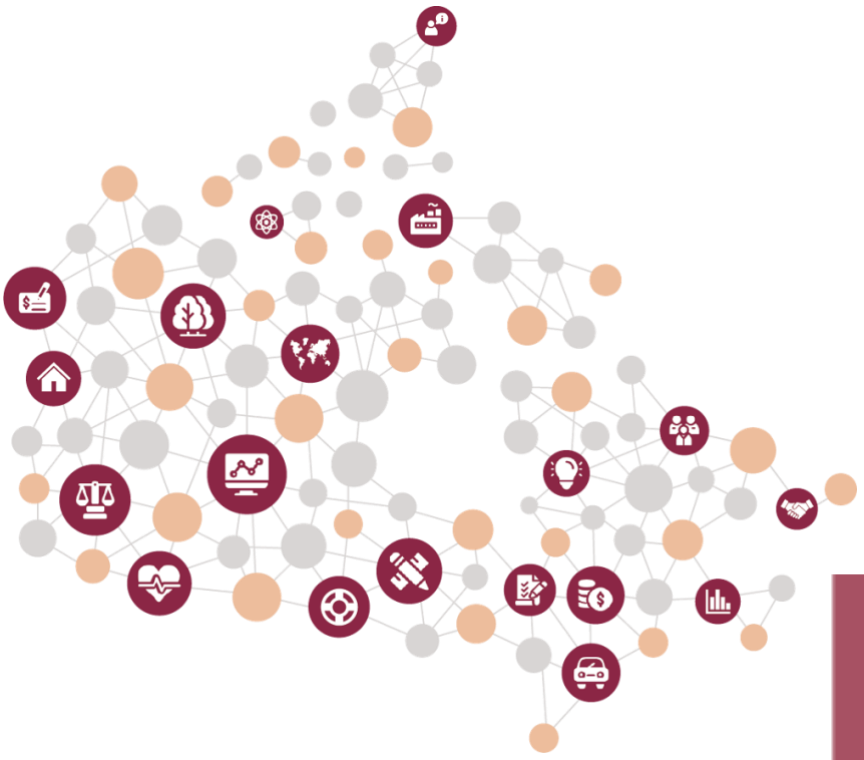
CIRANO

Allier savoir et décision



INTEROPÉRABILITÉ DES DONNÉES DU SECTEUR PUBLIC AU CANADA : BÂTIR UNE CAPACITÉ SOUVERAINE MUTUALISÉE AU SERVICE DES CITOYENS

ALAIN DUDOIT
ANNE-MARIE HUBERT
TONY LABILLOIS

PR 2026PR-06
POUR RÉFLÉXION

CIRANO
Allier savoir et décision

Les documents **Pour Réflexion** sont des documents publiés pour susciter échanges et commentaires et s'appuient sur des résultats de recherche. Ces documents sont sous la seule responsabilité des auteurs.

Reflection Papers are documents published to stimulate discussion and commentary, based on research findings. These documents are the sole responsibility of their authors.

Le CIRANO est un organisme sans but lucratif constitué en vertu de la Loi des compagnies du Québec. Le financement de son infrastructure et de ses activités de recherche provient des cotisations de ses organisations-membres, d'une subvention d'infrastructure du gouvernement du Québec, de même que des subventions et mandats obtenus par ses équipes de recherche.

CIRANO is a private non-profit organization incorporated under the Quebec Companies Act. Its infrastructure and research activities are funded through fees paid by member organizations, an infrastructure grant from the government of Quebec, and grants and research mandates obtained by its research teams.

Les partenaires du CIRANO – *CIRANO Partners*

Partenaires Corporatifs - Corporate Partners	**Partenaires gouvernementaux - Governmental partners**	**Partenaires universitaires - University Partners**
Autorité des marchés financiers	Ministère des Finances du Québec	École de technologie supérieure
Banque de développement du Canada	Ministère de l'Économie, de l'Innovation et de l'Énergie	École nationale d'administration publique
Banque du Canada	Innovation, Sciences et Développement Économique Canada	HEC Montréal
Banque Nationale du Canada	Ville de Montréal	Institut national de la recherche scientifique
Bell Canada		Polytechnique Montréal
BMO Groupe financier		Université Concordia
La Caisse		Université de Montréal
Énergir		Université de Sherbrooke
Hydro-Québec		Université du Québec
Intact Corporation Financière		Université du Québec à Montréal
Mouvement Desjardins		Université Laval
Power Corporation du Canada		Université McGill
Pratt & Whitney Canada		
VIA Rail Canada		

Le CIRANO collabore avec de nombreux centres et chaires de recherche universitaires dont on peut consulter la liste sur son site web. *CIRANO collaborates with many centers and university research chairs; list available on its website.*

Les idées et les opinions émises dans cette publication sont sous l'unique responsabilité des auteurs et ne représentent pas les positions du CIRANO ou de ses partenaires. *The observations and viewpoints expressed in this publication are the sole responsibility of the authors; they do not represent the positions of CIRANO or its partners.*

ISSN 2563-7266 (version en ligne)

Interopérabilité des données du secteur public au Canada : Bâtir une capacité souveraine mutualisée au service des citoyens

Alain Dudoit
Ambassadeur du Canada (ret).
Fellow invité CIRANO
Conseiller stratégique Global Advantage Consulting Group

Anne-Marie Hubert
Fellow invité CIRANO
Conseillère spéciale auprès de la fondation IFRS
Ancienne membre du Conseil consultatif mondial d'EY et du comité de direction canadien d'EY

Tony Labillois
Consultant en accessibilité, politiques publiques, leadership et données
Directeur général (retraité) chez Statistique Canada
Membre élu de l'Institut international de statistique

11 mai 2026

Pour citer ce document / To quote this document

Dudoit, A., Hubert, A-M. & Labillois, T. (2026). Interopérabilité des données du secteur public au Canada : Bâtir une capacité souveraine mutualisée au service des citoyens (2026PR-06, Pour réflexion, CIRANO). https://doi.org/10.54932/IWRY4867

Avant-propos et remerciements

Quatre publications CIRANO (listées ci bas) précèdent celle-ci. Elles s'inscrivent dans une trajectoire analytique cohérente, qui gagne progressivement en densité stratégique. Le point de départ (le rapport Bourgogne, d'octobre 2025) s'appuie sur un constat bien établi : la fragmentation des données entre les différents paliers de gouvernement (fédéral, provincial et territorial- FPT) entraîne des inefficacités, des doublons et des compartimentations persistantes. Ce constat initial a servi de socle à une requalification plus ambitieuse, dans laquelle les données cessent d'être perçues comme un simple enjeu de modernisation administrative pour devenir un actif stratégique, tandis que l'intelligence artificielle s'impose comme une véritable infrastructure.

Cette évolution conceptuelle ouvre elle-même sur une lecture en termes de souveraineté numérique, entendue non pas comme autosuffisance, mais comme capacité à maîtriser ses dépendances. À mesure que la réflexion progresse, le cadre analytique s'est déplacé vers le registre de la sécurité nationale. Les enjeux ne relèvent plus seulement de la performance administrative, mais de vulnérabilités systémiques, de dépendances critiques et de latences décisionnelles susceptibles d'affecter la capacité d'action du secteur public. Cette montée en puissance conduit logiquement à une prochaine étape, centrée sur la nécessité d'une capacité intégrée, articulant de manière cohérente la gouvernance, les infrastructures et les données.

Cette cinquième publication constitue ainsi une inflexion décisive : il ne s'agit plus d'analyser ni même de convaincre, mais d'opérationnaliser cette trajectoire à travers la proposition concrète d'un prototype d'accord-cadre fédéral-provincial-territorial FPT+ (incluant les premières nations et les municipalités) des données du secteur public et de l'adoption responsable de l'IA au Canada. L'accord FPT d'octobre 2025 sur la cybersécurité a établi un « périmètre défensif » (cybersécurité). Le prototype mis de l'avant dans notre projet de publication fait valoir que le maintien d'une posture défensive conduit à la fragmentation des systèmes : un cadre cyber unifié sans interopérabilité des données revient à disposer d'un réseau ferroviaire national sécurisé avec des rails de gabarit différents dans chaque province, c'est sécurisé, mais rien ne bouge ! Après l'entente FPT de 2025 sur la cybersécurité, qui a établi une position défensive unifiée pour les infrastructures du secteur public canadien, il est maintenant temps pour les gouvernements FPT de reconnaître que la sécurité est la base, mais que l'interopérabilité est l'accélérateur d'un secteur public FPT+ souverain, résilient et efficace.

1. RAPPORT BOURGOGNE Interopérabilité fédérale-provinciale des données et adoption de l'IA : Tirer parti de la dynamique fédérale-provinciale actuelle et du partenariat stratégique Canada-UE (https://doi.org/10.54932/AXET1370)
2. Souveraineté numérique et fédéralisme : architecture d'interopérabilité et gouvernance de l'IA au Canada (https://doi.org/10.54932/TDBZ9121)
3. Interopérabilité des données du secteur public au Canada et adoption responsable de l'IA : Synthèse stratégique et appel à l'action https://doi.org/10.54932/VOKC1489
4. Souveraineté numérique et intelligence artificielle au Canada : De la fragmentation des systèmes à la capacité stratégique intégrée du secteur public https://doi.org/10.54932/AFQN6960

Les auteurs tiennent à remercier Charles S. Morgan (associé chez McCarthy Tétrault et ancien président de l'*International Technology Law Association* — ITechLaw) dont la relecture du manuscrit a permis d'éclairer plusieurs dimensions clés de l'analyse. Nous sommes aussi reconnaissants à Alexis Bouffioux, coordonnateur des communications pour la vérification et la mise en page conformes aux normes de publication CIRANO. Ces commentaires et contributions ont enrichi la qualité et la pertinence de ce travail. Les auteurs cependant demeurent seuls responsables du contenu et de la présentation du rapport final.

Table des matières

Avant-propos et remerciements 4

Résumé/Abstract 7

Introduction : Une fenêtre d'action à ne pas manquer 9

Section 1 De la cybersécurité à l'interopérabilité : élargir le périmètre de la coopération FPT 11

1.2 Une dynamique de consolidation encore incomplète 11

1.3 Le déplacement du problème : de la sécurité à la circulation des données 11

1.4 De la protection à l'activation : une transformation de la logique publique 12

1.5 Les effets systémiques de la non-interopérabilité 12

1.6 L'interopérabilité comme infrastructure stratégique 13

1.7 Le rôle amplificateur de l'intelligence artificielle 13

1.8 Vers un fédéralisme opérationnel fondé sur la collaboration 14

1.9 Une question désormais politique 14

Section 2, Pourquoi un accord-cadre FPT est non seulement possible, mais nécessaire .. 15

2.1 Une transformation qui dépasse la modernisation administrative 15

2.2 Une dissociation entre vision stratégique et mise en œuvre 15

2.3 La fragmentation comme problème structurel 15

2.4 L'effet de seuil lié à l'intelligence artificielle 16

2.5 Les impacts concrets pour les citoyens 17

2.6 Un déficit d'architecture, non de capacité 17

2.7 Une pression internationale croissante 19

2.8 Une fenêtre d'opportunité réelle 19

2.9 L'accord-cadre comme condition de cohérence 19

2.10 L'interopérabilité : une gestion des risques contrôlée 20

2.11 Une nécessité stratégique, non optionnelle 21

Section 3, Ce que montre l'expérience internationale : un modèle fédéré fondé sur la confiance et les normes 22

3.1 Une démonstration de faisabilité, non un modèle à transposer 22

3.2 Le cas de l'Union européenne : une gouvernance structurée sans centralisation 22

3.3 Une logique opérationnelle fondée sur la réutilisation 23
3.4 Le cas australien : intégration stratégique des capacités 23
3.5 Des instruments concrets au service de la confiance 23
3.6 Le rôle des juridictions dans la dynamique fédérée 24
3.7 Le rôle structurant des API et des normes 24
3.8 L'apport analytique de l'OCDE 25
3.9 Les conditions de succès d'un modèle fédéré 26
3.10 Transition vers l'opérationnalisation 26
Section 4. Du prototype conceptuel à une base opérationnelle de discussion et négociation FPT 27
4.1 Une vision fédérée : rendre interopérable sans centraliser 27
4.2 Des principes structurants adaptés au fédéralisme canadien 28
4.3 Une architecture de gouvernance orientée vers la collaboration et l'exécution 28
4.4 Une innovation structurante : l'évaluation de l'interopérabilité 29
4.5 Des instruments opérationnels : expérimentation encadrée et accords d'échange . 30
4.6 Une mise en œuvre progressive et adaptable 31
4.7 Garanties juridiques et respect des compétences 31
4.8 Une base de discussion directement mobilisable pour l'action 32
Conclusion 33
De la faisabilité à la décision : vers un mandat explicite de négociation FPT 33
Annexe, Base de travail pour un instrument FPT d'interopérabilité des données et d'adoption responsable de l'IA 36
Sources et références 47

Résumé/Abstract

Français

Cet article soutient que le Canada se trouve à un point de bascule dans l'évolution de sa gouvernance numérique : les conditions sont désormais réunies pour passer d'une coopération intergouvernementale sectorielle à une capacité d'action coordonnée fondée sur l'interopérabilité des données publiques et l'adoption responsable de l'intelligence artificielle (IA).

S'appuyant sur le précédent structurant de l'accord fédéral–provincial–territorial (FPT) sur la cybersécurité conclu à Kananaskis en 2025, l'analyse montre que la protection des systèmes ne constitue qu'une première étape. La pleine valeur des investissements numériques dépend de la capacité des gouvernements à permettre une circulation sécurisée, gouvernée et ciblée des données entre juridictions. Dans ce contexte, l'interopérabilité n'apparaît pas comme un enjeu technique, mais comme une infrastructure stratégique conditionnant la performance économique, la qualité des services publics et la capacité d'anticipation du secteur public.

L'article met en évidence une contrainte structurelle : malgré l'existence de stratégies ambitieuses et de cas d'usage concrets en matière d'IA, la fragmentation des systèmes de données limite les gains potentiels et empêche l'émergence d'effets systémiques. Cette fragmentation constitue moins un déficit technologique qu'un déficit d'architecture institutionnelle et de mécanismes de confiance à l'échelle FPT. À partir d'une analyse comparative d'expériences internationales, notamment en Europe et en Australie, l'article démontre la faisabilité d'un modèle fédéré reposant sur des normes communes, des mécanismes de gouvernance partagée et une mutualisation ciblée des capacités, sans centralisation des données.

Sur cette base, il propose un prototype d'accord-cadre FPT conçu comme une base opérationnelle de concertation intergouvernementale. Cet avant-projet articule des principes structurants, une architecture de gouvernance, des instruments techniques et juridiques, ainsi que des mécanismes de mise en œuvre progressive. Il vise à concilier autonomie des juridictions et capacité d'action collective, en introduisant des dispositifs tels que l'évaluation de l'interopérabilité, les bacs à sable et des accords sectoriels d'échange de données.
L'article conclut que le Canada ne fait pas face à un déficit de diagnostic, mais à un impératif de mise en cohérence. Dans un environnement international marqué par la montée des dépendances technologiques et la centralité des données, la capacité à organiser ces dernières comme une architecture fédérée interopérable devient un déterminant stratégique de souveraineté, de résilience et de prospérité.

English
This paper argues that Canada has reached a tipping point in the evolution of its digital governance : the conditions are now in place to move from sectoral intergovernmental cooperation toward a coordinated capacity for action based on public data interoperability and the responsible adoption of artificial intelligence (AI).
Building on the precedent set by the 2025 federal-provincial-territorial (FPT) cybersecurity agreement concluded in Kananaskis, the analysis shows that securing systems is only a first step. The full value of digital investments now depends on governments' ability to enable the secure, governed, and targeted circulation of data across jurisdictions. In this context, interoperability should not be understood as a technical issue, but as a strategic infrastructure shaping economic performance, public service delivery, and the public sector's capacity to anticipate and act.

The paper identifies a structural constraint: despite ambitious strategies and concrete AI use cases, the fragmentation of public data systems limits potential gains and prevents the emergence of systems-wide effects. This fragmentation reflects not a technological deficit, but an institutional and governance gap, particularly in terms of trust mechanisms at the FPT level. Drawing on international experience, particularly from the European Union and Australia, the paper demonstrates the feasibility of a federated model based on shared standards, joint governance mechanisms, and targeted mutualization of capabilities, without centralizing data.

On this basis, it introduces a prototype FPT framework agreement designed as an operational foundation for intergovernmental negotiation. The proposal combines guiding principles, governance architecture, technical and legal instruments, and a phased implementation approach. It seeks to reconcile jurisdictional autonomy with collective capacity, notably through mechanisms such as interoperability assessments, regulatory sandboxes, and structured sectoral data-sharing agreements.

The paper concludes that Canada does not face a diagnostic gap, but a coordination imperative. In a global environment shaped by technological dependencies and the growing centrality of data, the ability to organize public data as a federated interoperable architecture is becoming a key determinant of sovereignty, resilience, and long-term prosperity.

Introduction : Une fenêtre d'action à ne pas manquer

Le Canada ne fait plus face à un déficit de vision en matière d'intelligence artificielle, mais à un déficit d'intégration de ses propres capacités publiques.

La réunion fédérale-provinciale territoriale de Kananaskis en 2025, marquée par la conclusion d'une entente sur la cybersécurité, a établi un précédent structurant : celui d'une capacité des gouvernements à agir collectivement face à des enjeux numériques désormais reconnus comme stratégiques. Depuis, les conditions politiques, technologiques et institutionnelles ont évolué de manière significative, au point de rendre possible une étape supplémentaire, le passage de la coopération sectorielle à une architecture fédérée.

Cette évolution repose sur des développements récents convergents. Le gouvernement du Canada vient de publier la Mise à jour économique du printemps de 2026 dans laquelle il présente sa vision de l'intelligence artificielle pour tous ; cette stratégie proposée « *aidera à accélérer l'adoption de l'IA par les petites et moyennes entreprises* ***et à transformer la prestation des services publics afin de mieux servir la population canadienne*** **.** Parallèlement, le portrait des usages de l'intelligence artificielle publié par le Gouvernement du Québec montre que ces technologies sont déjà en déploiement concret au sein des administrations publiques, avec une diversité de cas d'usage et une capacité d'innovation réelle.

La vision stratégique du gouvernement fédéral et une base d'expérimentation administrative tangible révèlent une dynamique claire. Ce qui fait défaut, toutefois, n'est ni la vision ni la capacité d'innovation, mais l'architecture permettant d'en assurer la cohérence. En l'absence d'une interopérabilité effective des données publiques à l'échelle fédérale, provinciale et territoriale, ces initiatives risquent de demeurer fragmentées, limitant leur impact systémique.
C'est précisément dans cet écart, entre ambition stratégique et capacité d'intégration que se situe la fenêtre d'action actuelle. Les conditions nécessaires à une transformation coordonnée sont désormais réunies : une reconnaissance politique des enjeux, des capacités techniques en émergence, et un précédent institutionnel démontrant la faisabilité d'une action collective. Dans ce contexte, la question n'est plus de savoir s'il faut agir, mais comment structurer cette action.

Le présent article propose de répondre à cette question en s'inscrivant dans la continuité de l'esprit de Kananaskis. Il avance que l'étape suivante ne consiste pas à multiplier les initiatives, mais à les relier. À cette fin, il propose un avant-projet d'accord-cadre fédéral–provincial–territorial (FPT) sur l'interopérabilité des données publiques et l'adoption de l'intelligence artificielle, comme une base opérationnelle de négociation.

Dans un environnement marqué par la fragmentation géopolitique, la montée des dépendances technologiques et la centralité croissante des données dans la capacité d'action des États, la capacité à organiser ces données comme un système cohérent devient un déterminant stratégique.

L’enjeu n’est plus seulement administratif ou technologique : il est désormais institutionnel, économique et, de plus en plus, lié à la souveraineté. Dans cette perspective, l’accord-cadre proposé ne constitue pas une option parmi d’autres. Il apparaît comme l’instrument permettant de transformer une convergence encore partielle en capacité d’action intégrée à l’échelle du Canada.

Le gouvernement fédéral s’apprête à lancer une stratégie structurée en matière d’intelligence artificielle ; les administrations publiques, notamment au Québec, en démontrent déjà les usages concrets. Ce qui fait défaut n’est ni la vision ni la capacité, mais l’architecture permettant d’en assurer la cohérence. Sans interopérabilité des données à l’échelle FPT, ces initiatives resteront fragmentées. L’accord-cadre envisagé dans ce rapport vise précisément à combler cette lacune structurelle. L’approche proposée s’inscrit explicitement dans une logique de fédéralisme collaboratif, où l’interopérabilité vise à renforcer la capacité d’action des juridictions sans en modifier les compétences ni en réduire l’autonomie décisionnelle, tout en protégeant la vie privée et le principe d’utilisation limitée des données.

À ce stade, l’objectif vise à favoriser l’émergence d’une structure organisationnelle collaborative capable de soutenir durablement l’interopérabilité des données, l’intégration éclairée de l’intelligence artificielle et l’amélioration continue de la prestation des services publics. Les conditions analytiques, institutionnelles et politiques nécessaires à ce passage apparaissent aujourd’hui largement réunies. Reste à en préciser les modalités de mise en œuvre de manière à en assurer la faisabilité et l’adhésion.

Cette logique de progression suppose enfin un ancrage juridique suffisamment clair pour soutenir la confiance entre les parties. L’accord envisagé intègre ainsi des garanties explicites visant à assurer sa compatibilité avec le cadre constitutionnel canadien et les régimes juridiques existants. Celles-ci participent également à la réduction des risques de perte de contrôle décisionnel, en assurant que les systèmes déployés demeurent ancrés dans des cadres juridiques explicites et contrôlables.

La participation des juridictions n’entraîne aucune modification de leurs compétences, et les modalités de mise en œuvre doivent être interprétées à la lumière des lois applicables, notamment en matière de protection de la vie privée, d’accès à l’information et de gestion des données. Ces garanties sont essentielles pour ancrer le projet d’accord envisagé dans une logique de collaboration respectueuse des responsabilités de chacun, et pour soutenir une appropriation progressive par les administrations concernées.

Section 1 De la cybersécurité à l'interopérabilité : élargir le périmètre de la coopération FPT

1.1 Un point d'inflexion : l'accord de Kananaskis comme précédent structurant

La signature de l'accord fédéral-provincial-territorial (FPT) sur la cybersécurité en octobre 2025, dans le contexte de la rencontre ministérielle de Kananaskis, constitue un point d'inflexion majeur dans l'évolution récente de la coopération intergouvernementale au Canada. Cet accord marque une reconnaissance explicite du caractère systémique des risques numériques et de la nécessité d'une réponse coordonnée à l'échelle de l'ensemble du secteur public.

Au-delà de sa portée immédiate, cet accord introduit un précédent institutionnel structurant : celui d'une capacité des gouvernements FPT à s'entendre sur des enjeux technologiques critiques touchant simultanément la sécurité nationale, la résilience des infrastructures et la continuité des services publics. Il établit ainsi un socle commun, un « périmètre défensif partagé », à partir desquels une évolution vers une capacité plus intégrée devient logique et souhaitable.

1.2 Une dynamique de consolidation encore incomplète

Dans les mois qui ont suivi cet accord, plusieurs développements sont venus en consolider la portée et en révéler les implications opérationnelles. Les mécanismes de collaboration entre dirigeants principaux de l'information (DPI), la mise en place du Bureau de la transformation numérique et les initiatives en matière d'infrastructures numériques ont contribué à renforcer une dynamique intergouvernementale déjà existante, jusque-là fragmentée. Ces avancées demeurent encore partielles, elles témoignent d'une capacité réelle des gouvernements à aligner leurs approches autour d'objectifs communs lorsque le cadre politique et stratégique est clairement établi.

1.3 Le déplacement du problème : de la sécurité à la circulation des données

Parallèlement, l'accélération des travaux liés à l'intelligence artificielle, notamment dans le contexte de l'évolution du cadre législatif canadien en matière de données et d'IA, a mis en évidence l'importance croissante de la circulation sécurisée des données entre juridictions. De même, les priorités économiques et sociales identifiées dans les politiques publiques récentes, qu'il s'agisse de productivité, de logement, de mobilité de la main-d'œuvre ou de gestion des infrastructures, reposent de plus en plus explicitement sur la capacité à mobiliser des données interopérables à l'échelle du système.

1.4 De la protection à l'activation : une transformation de la logique publique

Ces développements convergents contribuent à déplacer la question de l'interopérabilité du registre technique vers celui de la capacité d'action collective. Ils rendent plus visible une réalité déjà présente : les systèmes existent, les données existent et les investissements sont en cours. Leur pleine valeur demeure conditionnée par leur capacité à être mobilisés de manière coordonnée entre les juridictions. Cette évolution repose sur une distinction fondamentale. La cybersécurité vise à protéger les systèmes. L'interopérabilité des données vise à activer leur potentiel.

Au-delà de cette distinction fonctionnelle, l'enjeu réel est d'ordre économique, social et humain. La protection des systèmes contribue à la sécurité des institutions. L'activation des données conditionne, quant à elle, la capacité des gouvernements à améliorer concrètement la vie des citoyens, en renforçant la qualité et la continuité des services publics, en soutenant la prospérité économique, en facilitant la mobilité et en garantissant l'exercice effectif des droits dans un environnement numérique intégré. Ainsi, la cybersécurité protège l'intégrité des systèmes. L'interopérabilité permet d'en traduire le potentiel en valeur publique. Autrement dit, la sécurité constitue une condition nécessaire, non suffisante, de la capacité d'action publique dans un environnement numérique. Un système parfaitement sécurisé, cloisonné demeure structurellement limité dans sa capacité à produire de la valeur collective, à soutenir la prise de décision et à répondre efficacement à des enjeux transversaux.

1.5 Les effets systémiques de la non-interopérabilité

Cette limite apparaît de manière particulièrement claire dans les domaines à forte intensité de données, comme la santé, interventions d'urgence, infrastructures critiques, mobilité de la main-d'œuvre où la performance dépend directement de la capacité à partager, à accéder, à croiser et à exploiter l'information entre juridictions. Dans ces contextes, l'absence d'interopérabilité crée des frictions invisibles, déterminantes : délais décisionnels, duplication des efforts, incohérences opérationnelles et perte de valeur des données existantes. Nous trouvons un cas concret de ces impacts dans l'analyse transversale et multidisciplinaire des défis et des possibilités concernant l'interopérabilité et le partage des données dans le cadre de la stratégie de données sur le transport intermodal et le commerce du « Corridor commercial des Grands Lacs et du Saint-Laurent » (CCGLSL). La taille et la portée de ce corridor commercial n'ont d'égal que la complexité de ses systèmes multimodaux de transport de marchandises et l'urbanisation croissante des deux côtés de la frontière canado-américaine. Cette complexité est exacerbée par le manque d'interopérabilité des données et de collaborations efficaces entre les différents intervenants au sein des diverses juridictions et entre eux.

L'interopérabilité des données peut être comprise comme l'extension fonctionnelle de la cybersécurité. Elle permet l'activation du potentiel des infrastructures désormais sécurisées. Cette articulation positionne la démarche comme la continuité logique d'un engagement déjà pris.

1.6 L’interopérabilité comme infrastructure stratégique

Ce passage de la protection à l’activation correspond également à une transformation plus large du rôle des données dans l’action publique. Celles-ci ne peuvent plus être considérées uniquement comme des ressources administratives ; elles sont des composantes essentielles d’une infrastructure stratégique, au même titre que les réseaux énergétiques ou de transport. Dans ce cadre, leur capacité à circuler de manière efficace, sécurisée et contrôlée devient un déterminant direct de la performance globale du système.

1.7 Le rôle amplificateur de l’intelligence artificielle

L’intelligence artificielle (IA) accentue encore cette dynamique. En tant qu’infrastructure de traitement et de valorisation des données, elle dépend directement de leur qualité, de leur accessibilité et de leur compatibilité. Sans interopérabilité, les applications d’IA restent confinées à des périmètres restreints, limitant leur impact et leur capacité à produire des gains systémiques. À l’inverse, un environnement de données interopérables permet le développement d’applications transversales à fort effet de levier, notamment dans les domaines de la planification, de la gestion des risques et de l’optimisation des services publics.

Cette capacité demeure toutefois conditionnée par des limites juridiques, juridictionnelles et institutionnelles particulièrement importantes dans le contexte fédéral canadien. La circulation et la réutilisation des données publiques doivent en effet s’inscrire dans le respect des compétences des juridictions participantes, des régimes applicables en matière de protection de la vie privée et des principes encadrant l’utilisation des renseignements personnels. L’interopérabilité des données du secteur public repose sur des mécanismes de gouvernance, de confiance et de traçabilité permettant d’assurer que les échanges demeurent proportionnés, sécurisés et conformes aux finalités autorisées. L’enjeu central réside dans la capacité à construire une infrastructure de confiance suffisamment robuste pour soutenir une collaboration intergouvernementale durable.

La combinaison de cybersécurité et d’interopérabilité représente un cheminement unifié vers une capacité publique partagée : la cybersécurité renforce la confiance, l’interopérabilité permet la circulation, et l’IA génère la valeur.

1.8 Vers un fédéralisme opérationnel fondé sur la collaboration

L'élargissement du périmètre de la coopération FPT vers l'interopérabilité des données apparaît comme une évolution naturelle, fondée sur des acquis récents et compatible avec les principes du fédéralisme canadien. Il s'agit de créer les conditions permettant leur collaboration effective autour d'objectifs communs. Cette approche s'inscrit dans une logique de fédéralisme opérationnel, où la coopération ne repose pas sur la centralisation des systèmes, mais sur leur capacité à interagir selon des règles partagées. Elle repose sur une mutualisation consensuelle ciblée, des normes, des interfaces, des mécanismes de confiance, plutôt que sur une intégration institutionnelle.

En ce sens, l'interopérabilité ne doit pas être perçue comme un projet technique, mais comme une infrastructure stratégique de collaboration concrète. Elle constitue le mécanisme par lequel les capacités existantes des différentes juridictions peuvent être mobilisées de manière cohérente, efficace et actuelle pour répondre à des enjeux communs.

1.9 Une question désormais politique

L'expérience récente de la cybersécurité démontre que ce type de collaboration est possible. Elle suggère également que les conditions politiques et institutionnelles nécessaires à une telle évolution sont désormais réunies. Il s'agit désormais de préciser les modalités de mise en œuvre et la pérennité de cette trajectoire vers l'interopérabilité des données du secteur public. La question n'est plus seulement technique ou administrative ; elle est explicitement politique : comment organiser, à l'échelle des systèmes, les conditions permettant aux gouvernements d'agir de manière cohérente, sécurisée et efficace dans un environnement numérique partagé.

Section 2, Pourquoi un accord-cadre FPT est non seulement possible, mais nécessaire

2.1 Une transformation qui dépasse la modernisation administrative

La transformation numérique du secteur public au Canada ne peut plus être envisagée comme une juxtaposition d'initiatives sectorielles ou de modernisation administrative. Elle s'inscrit désormais dans un environnement marqué par l'accélération de l'intelligence artificielle, la montée des dépendances technologiques et la centralité croissante des données dans la capacité d'action des gouvernements. La fragmentation actuelle des systèmes de données publics, entre juridictions, secteurs et institutions, est un facteur limitant de la performance économique, de la qualité des services publics et, de plus en plus, de la capacité du secteur public à anticiper et à agir de manière cohérente.

2.2 Une dissociation entre vision stratégique et mise en œuvre

Les développements récents confirment empiriquement le diagnostic posé en introduction. La mise à jour économique du Gouvernement du Canada formalise une vision structurée de l'intelligence artificielle comme levier de transformation économique, institutionnelle et démocratique. Elle met notamment l'accent sur la confiance, l'adoption à grande échelle, la souveraineté des infrastructures et le développement d'alliances internationales. Parallèlement, le portrait des utilisations de l'intelligence artificielle dans l'administration publique du Québec offre une lecture opérationnelle de cette transformation, en documentant une diversité de cas d'usage déjà déployés au sein des organismes publics. Cette combinaison est éloquente. Elle montre que le Canada se situe dans une phase intermédiaire caractérisée par une dissociation entre vision et exécution.

C'est précisément cette dissociation qui constitue le problème structurel auquel le présent article s'attaque. En l'absence d'une interopérabilité effective des données publiques à l'échelle fédérale, provinciale et territoriale, ces initiatives demeurent fragmentées et ne peuvent produire les effets systémiques attendus. Si ces initiatives ont permis des progrès réels, elles ne permettent pas de produire une capacité distribuée à l'échelle du système FPT.

2.3 La fragmentation comme problème structurel

Les approches actuelles reposent encore largement sur des logiques sectorielles, institutionnelles ou technologiques cloisonnées. Cette situation engendre plusieurs effets structurants. D'abord, une fragmentation informationnelle qui limite la visibilité sur les dynamiques économiques, sociales et territoriales, et complique la collaboration des interventions publiques. Ensuite, une duplication des efforts et des investissements, chaque juridiction développant ses propres solutions, souvent incompatibles entre elles, ce qui réduit les gains d'efficacité potentiels.

La fragmentation actuelle n'élimine pas les risques, elle les rend simplement moins visibles et plus difficiles à gérer. Des systèmes cloisonnés, non coordonnés et reposants sur des architectures hétérogènes produisent déjà des vulnérabilités importantes : incohérences décisionnelles, angles morts informationnels, dépendances implicites et incapacité à anticiper les effets systémiques.

L'analyse des risques liés à l'usage de l'intelligence artificielle dans les services publics met en lumière des enjeux réels et documentés. Les cas récents, au Canada comme à l'international, démontrent que des systèmes automatisés mal conçus peuvent produire des erreurs significatives et, dans certains cas, des conséquences humaines graves. Toutefois, ces exemples appellent une lecture plus systémique. Les défaillances observées ne résultent pas principalement de l'intelligence artificielle en tant que telle, mais des conditions dans lesquelles elle est déployée. Elles révèlent moins une approche d'intégration uniforme des systèmes qu'une fragmentation persistante des données, des processus et des mécanismes de gouvernance.

Dans un environnement où les données sont cloisonnées, où les normes sont hétérogènes et où les mécanismes de validation sont limités, l'IA agit comme un amplificateur des incohérences existantes. À l'inverse, dans un écosystème fondé sur l'interopérabilité, des règles communes et des mécanismes de confiance, elle peut devenir un instrument de cohérence, de détection des erreurs et d'amélioration continue. La question centrale n'est donc pas de savoir s'il faut ralentir l'adoption de l'IA dans les services publics, mais de déterminer dans quelle architecture institutionnelle et informationnelle elle est déployée.

2.4 L'effet de seuil lié à l'intelligence artificielle

Cette dynamique crée un effet de seuil. En deçà d'un certain niveau de mise en relation des données, les gains associés à l'IA demeurent marginaux. Au-delà de ce seuil, ils deviennent exponentiels. La fragmentation actuelle empêche le secteur public canadien de franchir ce seuil à l'échelle du système. De plus, cette dynamique réduit rapidement les marges de manœuvre des systèmes publics qui ne parviennent pas à relier leurs données à l'échelle requise, créant un écart croissant entre les capacités potentielles et les capacités réellement mobilisées.

Cette évolution renforce également la nécessité d'un cadre commun de gouvernance permettant d'encadrer la circulation et la réutilisation des données entre juridictions. Dans le contexte fédéral canadien, l'augmentation des capacités d'échange et d'exploitation des données ne peut reposer sur des mécanismes ad hoc ou sur une simple compatibilité technique. Elle doit s'appuyer sur des règles communes assurant la conformité aux cadres juridiques applicables, le respect des compétences des juridictions participantes, ainsi que la protection de la vie privée et des renseignements personnels. En l'absence d'une telle architecture de confiance, la multiplication des échanges de données risque d'accentuer les incertitudes juridiques, les asymétries de gouvernance et les risques de fragmentation, limitant ainsi la capacité de développer des usages de l'intelligence artificielle à l'échelle du système public canadien.

2.5 Les impacts concrets pour les citoyens

Ces limites entraînent des répercussions directes sur les citoyens. Elles se manifestent par des parcours administratifs fragmentés, des services publics discontinus et des délais dans l'accès à des prestations ou à des interventions essentielles. Dans des domaines comme la santé, l'emploi ou les services sociaux, l'absence d'interopérabilité peut entraîner des ruptures d'information qui affectent la qualité des services, la rapidité des interventions et, ultimement, la qualité de vie des personnes concernées. À l'inverse, une meilleure circulation des données permettrait d'offrir des services plus fluides, mieux adaptés aux besoins des citoyens et plus cohérents d'une juridiction à l'autre. L'accélération des transformations liées à l'intelligence artificielle exerce une pression supplémentaire sur les systèmes existants. L'IA repose sur l'accès à des ensembles de données vastes, diversifiés et de haute qualité. Elle amplifie les écarts entre les organisations capables de mobiliser ces données et celles qui restent confinées à des silos informationnels.

Cette dépendance structurelle aux données ne saurait toutefois être dissociée d'autres conditions tout aussi déterminantes pour une mise en œuvre soutenable.
Au-delà des infrastructures et de l'accès aux données, la capacité du secteur public à tirer pleinement parti de l'intelligence artificielle repose également sur la disponibilité des talents et sur le maintien d'un haut niveau de confiance dans les modalités de son déploiement. Cette dimension est structurante. Elle conditionne leur acceptabilité sociale et institutionnelle.

Le développement des compétences, l'accompagnement des transitions professionnelles et l'intégration de principes clairs en matière d'usage responsable de l'IA apparaissent comme des leviers complémentaires à l'interopérabilité des données. Ils contribuent à ancrer cette transformation dans une trajectoire à la fois performante et soutenable, en assurant que les gains associés à l'IA s'inscrivent dans une logique de création de valeur partagée et de confiance durable.

2.6 Un déficit d'architecture, non de capacité

Une exposition accrue aux dépendances technologiques externes, dans la mesure où l'absence de masse critique et de collaboration limite la capacité de développer et d'exploiter des infrastructures et des systèmes à l'échelle de la fédération. Ces limites relèvent avant tout un déficit d'architecture. Elles traduisent l'absence d'un cadre permettant de relier les initiatives existantes dans une logique cohérente au bénéfice des citoyennes et citoyens. Les travaux antérieurs ont également mis en évidence que les principaux obstacles à l'interopérabilité sont de nature politique. Les technologies requises, telles que les normes ouvertes, les API sécurisées et les architectures infonuagiques, sont facilement accessibles et bien comprises.

Ce qui fait défaut, c'est un cadre permettant leur adoption coordonnée à l'échelle intergouvernementale. L'interopérabilité repose moins sur des choix technologiques que sur des mécanismes de confiance : normes partagées, règles communes, dispositifs de conformité et de gouvernance adaptés. Cette dimension de confiance est d'autant plus déterminante que la protection de la vie privée constitue un enjeu central et structurant de l'action publique dans l'environnement numérique contemporain. Cette dimension est particulièrement pertinente dans le contexte canadien, où la diversité des juridictions exige des solutions compatibles avec un haut degré d'autonomie institutionnelle.

Les conclusions de l'enquête conjointe menée par le Commissaire à la protection de la vie privée du Canada et ses homologues provinciaux du Québec, de la Colombie-Britannique et de l'Alberta confirment que l'intégration croissante de l'intelligence artificielle dans les services publics et privés exige non seulement le respect des cadres juridiques existants, mais leur adaptation continue afin de garantir une protection effective des renseignements personnels.

L'un des enseignements majeurs de cette enquête conjointe réside dans le fait que la protection de la vie privée ne doit pas être envisagée comme une contrainte à l'innovation, mais comme la condition même de son déploiement responsable. En l'absence de garanties robustes, la confiance des citoyens, et, par extension, la légitimité des systèmes demeure fragile.

L'interopérabilité des données ne peut être conçue indépendamment des exigences de protection de la vie privée. Elle doit au contraire s'appuyer sur des mécanismes renforcés de gouvernance, d'évaluation et de sécurisation, permettant d'assurer que la circulation accrue des données s'accompagne d'un niveau de protection au moins équivalent, sinon supérieur, à celui des systèmes cloisonnés.

L'enjeu n'est donc pas d'arbitrer entre interopérabilité et protection de la vie privée, mais de concevoir une architecture dans laquelle ces deux dimensions se renforcent mutuellement. À cet égard, l'établissement d'un cadre FPT structuré constitue précisément un levier permettant d'assurer cette cohérence, en remplaçant des pratiques fragmentées par des approches coordonnées, auditables et évolutives.

Dans le cadre juridique canadien, le principe d'utilisation limitée des données, selon lequel les renseignements ne peuvent être utilisés qu'à des fins déterminées, légitimes et encadrées, est souvent perçu comme un frein à la circulation des données entre juridictions. Cette lecture, bien que compréhensible, est incomplète. En réalité, ce principe ne constitue pas un obstacle à l'interopérabilité. Il en définit les conditions de possibilité.

La pluralité des régimes juridiques et la sensibilité accrue des enjeux de protection de la vie privée, l'absence d'un cadre commun transforme l'utilisation limitée en facteur de fragmentation : multiplication des interprétations, complexité des échanges, sous-utilisation des données disponibles. À l'inverse, lorsqu'il est intégré dans une architecture de gouvernance partagée, ce même principe d'utilisation limitée des données devient un levier structurant.

Il permet d'encadrer la réutilisation des données de manière explicite et traçable ; assurer la compatibilité des usages entre juridictions ; renforcer la confiance institutionnelle et publique et sécuriser juridiquement les échanges intergouvernementaux.

L'utilisation limitée des données ne doit pas être envisagée comme une restriction, mais comme une infrastructure de confiance indispensable à toute interopérabilité durable. L'établissement d'un cadre FPT d'interopérabilité des données du secteur public est un préalable à une utilisation responsable et efficace de l'intelligence artificielle. Sans une telle architecture, les risques identifiés sont susceptibles de se multiplier. Avec elle, ils peuvent être structurés, encadrés et progressivement réduits.

2.7 Une pression internationale croissante

Par ailleurs, les transformations en cours dans l'environnement international renforcent cette pression. La montée en puissance de modèles d'interopérabilité à grande échelle, notamment en Europe, montre qu'il est possible de concilier gouvernance fédérée, respect des juridictions et intégration des systèmes. Ces expériences contribuent à lever une partie des objections politiques traditionnellement associées à ce type de démarche.

En l'absence d'un cadre structurant commun, chaque initiative doit définir ses propres règles, ses propres normes et ses propres mécanismes de gouvernance. Cette situation entraîne une multiplication des solutions incompatibles entre elles, renforçant paradoxalement la fragmentation qu'elles cherchent à réduire.

2.8 Une fenêtre d'opportunité réelle

Si la nécessité d'une action collaborative FPT apparaît aujourd'hui clairement, sa faisabilité repose sur plusieurs facteurs convergents. Sur le plan politique, le précédent établi par la coopération en matière de cybersécurité démontre qu'une action collective est possible lorsque les enjeux sont reconnus comme stratégiques. Sur le plan technologique, la maturité croissante des normes, des architectures infonuagiques et des outils d'interopérabilité rend techniquement réalisable ce qui ne l'était pas il y a encore quelques années. Sur le plan institutionnel, la multiplication d'initiatives au niveau fédéral et provincial peut servir de base sur laquelle construire une architecture fédérée.

2.9 L'accord-cadre comme condition de cohérence

L'établissement d'un accord-cadre fédéral–provincial–territorial apparaît non pas comme une extension des politiques existantes, mais comme la condition de leur cohérence et de leur mise en œuvre effective. Il permettrait de transformer une accumulation d'initiatives en une capacité structurée, capable de produire des effets à l'échelle du système.

2.10 L’interopérabilité : une gestion des risques contrôlée

Le discours de Mark Carney à Davos a agi comme un révélateur stratégique. Il ne s’est pas limité à décrire une transformation économique globale, mais a mis en évidence une contrainte structurante pour l’action publique contemporaine : l’incapacité croissante des États à gérer des risques systémiques sans coordination renforcée, sans normes communes et sans accès effectif à des données exploitables.

Son approche repose sur une séquence claire : reconnaître les risques, agir de manière cohérente, établir des cadres communs et réduire les vulnérabilités structurelles. Cette logique dépasse les marchés financiers ou le climat. Elle s’applique directement à la gouvernance publique des données. Dans ses travaux antérieurs à l’international sur les risques climatiques, Marc Carney insiste sur un principe fondamental : sans données accessibles, comparables et fiables, il est impossible d’anticiper les chocs, d’orienter les décisions et d’assurer une transition ordonnée. Cette idée trouve une résonance directe dans le contexte canadien.

Les défis actuels, qu’ils soient économiques, sociaux ou environnementaux, partagent une caractéristique commune : ils nécessitent des décisions coordonnées fondées sur des données distribuées entre juridictions.

Or, au Canada, ces données existent, mais leur fragmentation limite leur utilisation à l’échelle du système. L’enjeu n’est donc pas la production d’information, mais sa mise en relation dans des conditions sécurisées, gouvernées et interopérables. Dans cette perspective, l’interopérabilité des données publiques peut être comprise comme une infrastructure de gestion des risques collectifs. Elle permet de transformer des informations dispersées en capacité d’anticipation partagée, de soutenir la cohérence des interventions publiques et de réduire les asymétries d’information entre juridictions. Ainsi, l’appel du premier ministre Carney à des normes communes, à des mécanismes de coordination et à des institutions capables de piloter l’action collective trouve une traduction concrète dans le contexte FPT : la mise en place d’un cadre structuré d’interopérabilité des données.

Sans une telle architecture, les ambitions stratégiques en matière d’intelligence artificielle, de transition économique ou de résilience systémique risquent de demeurer limitées par une contrainte fondamentale : l’incapacité à organiser les données comme un actif collectif mobilisable à l’échelle du pays.

2.11 Une nécessité stratégique, non optionnelle

La question n'est donc plus de savoir si une meilleure collaboration des données publiques est souhaitable, mais si le Canada peut se permettre de ne pas la réaliser. Dans un environnement où la capacité à comprendre, anticiper et agir repose de plus en plus sur la qualité et la quantité des données probantes, l'interopérabilité FPT apparaît comme une condition structurante de l'action publique. Elle constitue le chaînon manquant entre des stratégies désormais établies et leur traduction en résultats concrets. C'est dans cette perspective que la section suivante examine les expériences internationales, afin d'éclairer les modalités concrètes par lesquelles une telle architecture peut être conçue et mise en œuvre dans un contexte fédéré.

L'enjeu n'est pas de choisir entre intégration et prudence, mais de concevoir une architecture d'interopérabilité capable d'intégrer explicitement la gestion de ces risques. Cela suppose de passer d'une accumulation de systèmes à une gouvernance consciente de leurs interactions. C'est précisément dans cette optique que l'établissement d'un accord-cadre FPT prend tout son sens. Loin d'accélérer des dynamiques non maîtrisées, il permettrait au contraire de rendre explicites les interdépendances entre systèmes ; d'encadrer les modalités d'échange et d'utilisation des données ; et de structurer une capacité collective d'anticipation et de gestion des risques.

Cette approche progressive apparaît également pertinente dans des contextes caractérisés par une forte diversité institutionnelle, notamment en ce qui concerne les relations avec les Premières Nations, où des démarches fondées sur l'expérimentation et la coconstruction pourraient constituer un levier privilégié.

Les conditions nécessaires à cette exploration apparaissent aujourd'hui réunies : convergence analytique, précédent institutionnel en matière de cybersécurité, maturité technologique et pression croissante liée à l'IA. Cette conjonction crée une fenêtre d'opportunité rare, dans laquelle l'élaboration d'un instrument structurant devient non seulement nécessaire, mais possible. Cette évolution s'inscrit dans une dynamique déjà observable à l'échelle internationale, où plusieurs juridictions ont entrepris de structurer l'interopérabilité des données dans des cadres fédérés fondés sur la confiance, les normes et la gouvernance partagée.

Section 3, Ce que montre l'expérience internationale : un modèle fédéré fondé sur la confiance et les normes

3.1 Une démonstration de faisabilité, non un modèle à transposer

L'expérience internationale ne doit pas être lue ici comme un modèle à transposer, mais comme une démonstration de faisabilité. Elle montre qu'il est possible de bâtir une gouvernance de l'interopérabilité qui respecte l'autonomie des juridictions tout en permettant la circulation sécurisée des données, la réutilisation des solutions et la production de capacités communes. À cet égard, les expériences de l'Union européenne et de l'Australie sont particulièrement instructives, non parce qu'elles seraient identiques au cas canadien, mais parce qu'elles confirment qu'un cadre fédéré peut être à la fois souple, robuste et politiquement acceptable. Cette lecture est cohérente avec les travaux antérieurs de CIRANO, qui ont déjà présenté l'interopérabilité comme une infrastructure stratégique, et non comme un simple ajustement technique.

3.2 Le cas de l'Union européenne : une gouvernance structurée sans centralisation [1]

Dans l'Union européenne, l'adoption de l'Interoperable Europe Act a institutionnalisé une coopération renforcée en matière d'interopérabilité du secteur public à l'échelle transfrontalière. Le portail Interoperable Europe présente cette initiative comme un mécanisme stratégique de coopération pour l'ensemble de l'Union, tandis que l'Interoperable Europe Board réunit des représentants de haut niveau des États membres et de la Commission européenne pour coordonner l'interopérabilité des services publics au-delà des frontières nationales. Le cadre européen met ainsi en place une gouvernance partagée, sans centralisation excessive, mais avec une capacité claire d'orientation, de suivi et d'alignement stratégique. Le règlement est en vigueur depuis le 11 avril 2024, ce qui en fait une référence récente et concrète pour toute réflexion sur la gouvernance des données dans un contexte fédéré.

[1] *Pour en savoir sur :*

- *L'expérience des espaces communs de données, vous pouvez consulter cette publication CIRANO de 2023 : https://doi.org/10.54932/RYHT5065 ; la partie 3 du Rapport Bourgogne d'octobre 2025 : https://doi.org/10.54932/AXET1370*
- *Règlement (UE) 2024/903 du Parlement européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (règlement pour une Europe interopérable) :*
  - *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R0903*
  - *https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf*

Dans l'Union européenne, l'adoption de l'Interoperable Europe Act a institutionnalisé une coopération renforcée en matière d'interopérabilité du secteur public à l'échelle transfrontalière. Le portail Interoperable Europe présente cette initiative comme un mécanisme stratégique de coopération pour l'ensemble de l'Union, tandis que l'Interoperable Europe Board réunit des représentants de haut niveau des États membres et de la Commission européenne pour coordonner l'interopérabilité des services publics au-delà des frontières nationales. Le cadre européen met ainsi en place une gouvernance partagée, sans centralisation excessive, mais avec une capacité claire d'orientation, de suivi et d'alignement stratégiques. Le règlement est en vigueur depuis le 11 avril 2024, ce qui en fait une référence récente et concrète pour toute réflexion sur la gouvernance des données dans un contexte fédéré.

3.3 Une logique opérationnelle fondée sur la réutilisation

Ce qui est particulièrement pertinent pour le Canada n'est pas seulement l'existence d'un cadre européen, mais la manière dont ce cadre organise la coopération. L'Union ne cherche pas à uniformiser ses administrations ; elle cherche à rendre leurs interactions possibles, prévisibles et réutilisables. Le portail européen insiste d'ailleurs sur l'importance d'identifier les besoins, d'expérimenter des solutions, puis de déployer celles qui peuvent être réutilisées à grande échelle. Les solutions recommandées par le Board sont sélectionnées selon leur utilité pour les usagers, leur réutilisabilité, leur sécurité, leur protection des données, leur ouverture et leur durabilité. Autrement dit, la gouvernance européenne de l'interopérabilité repose sur une logique de normes communes consensuelles et de mutualisation sélective, plutôt que sur une logique de contrôle centralisé.

3.4 Le cas australien : intégration stratégique des capacités

L'expérience australienne est également éclairante, mais pour des raisons légèrement différentes. L'Australie a explicitement intégré l'interopérabilité des données, la sécurité numérique et l'expérience citoyenne dans une même trajectoire de modernisation de l'État. Sa Data and Digital Government Strategy fixe une vision à l'horizon 2030 : offrir des services publics simples, sécurisés et connectés, à l'aide de capacités de données et de services numériques de classe mondiale.
Dans les documents de mise en œuvre, le gouvernement australien précise que l'échange sécurisé de données soutient à la fois l'interopérabilité, la réduction des doublons, les flux d'information fiables entre entités publiques et l'amélioration de l'expérience des usagers. L'architecture publique australienne associe ainsi directement la confiance, l'efficacité et l'interopérabilité.

3.5 Des instruments concrets au service de la confiance

L'Australie a également renforcé cette logique par des instruments plus précis. Le gouvernement a indiqué que le Digital ID Act 2024 établit, depuis le 1er décembre 2024, des normes nationales cohérentes pour la vérification d'identité, afin de rendre les interactions en ligne plus simples et plus sûres pour les personnes. Le même ensemble d'outils publics insiste sur le fait que l'augmentation des capacités de partage de données doit s'accompagner de garanties robustes de protection de la vie privée, de sécurité et de confiance publique.

L’expérience australienne présente un intérêt particulier dans le contexte canadien en raison de l’importance accordée à la confiance numérique comme condition de l’interopérabilité. Le Digital ID Act 2024 repose sur l’établissement de normes communes permettant une vérification sécurisée, cohérente et interopérable des interactions numériques entre administrations, organisations et citoyens.
Cette approche trouve un écho croissant au Canada à travers les travaux du Conseil canadien de l’identification et de l’authentification numériques (CCIAN/DIACC), qui réunit gouvernements, entreprises et organisations afin de développer des cadres communs de confiance numérique. Bien que cette initiative demeure principalement volontaire et collaborative, elle démontre que le Canada dispose déjà d’un écosystème institutionnel et technique capable de soutenir des mécanismes FPT+ d’identification, d’authentification et de vérification compatibles avec une architecture interopérable des données publiques.

Le parallèle entre ces deux expériences est particulièrement éclairant. Il suggère que l’enjeu canadien réside dans l’absence d’un cadre structurant permettant de relier les initiatives des différentes juridictions dans une logique cohérente à l’échelle FPT. L’identité numérique est une composante essentielle d’une infrastructure de confiance plus large, nécessaire à la circulation sécurisée des données, à la protection de la vie privée et au développement responsable des usages de l’intelligence artificielle.

3.6 Le rôle des juridictions dans la dynamique fédérée

Plus encore, les consultations ayant mené à la stratégie australienne montrent que les États et territoires ont eux-mêmes appelé à davantage de partage bidirectionnel des données, à des approches nationales communes et à des infrastructures partagées pour améliorer les services aux citoyens. Cette combinaison est importante. Elle montre qu’une gouvernance fédérée peut être portée non seulement par le centre, mais aussi par les juridictions participantes lorsqu’elles y voient un gain concret pour les personnes et pour l’efficacité de l’action publique. Cette collaboration s’inscrit dans le respect des compétences des juridictions participantes, de la protection de la vie privée et des mécanismes de confiance nécessaires à la circulation des données.

3.7 Le rôle structurant des API et des normes

L’Australie apporte aussi un enseignement utile sur la place des API, des normes de réutilisation et du principe « tell us once ». Sa stratégie publique précise que les interfaces de programmation doivent favoriser l’efficacité, la réutilisation, la réduction du risque et l’interopérabilité entre systèmes, tout en soutenant le passage à des services plus fluides pour les usagers. Cette approche rejoint directement l’idée, déjà présente dans les travaux CIRANO précédents, selon laquelle la mutualisation ne doit pas être pensée comme une fusion des administrations, mais comme une capacité commune à faire circuler l’information de manière sécurisée, gouvernée, efficace et utile.

3.8 L’apport analytique de l’OCDE

Au-delà de ces deux exemples, l’OCDE fournit un cadre de lecture particulièrement utile. L’Organisation souligne que l’accès aux données et leur partage peuvent maximiser la valeur sociale et économique de la réutilisation des données, tout en nécessitant des cadres de gouvernance capables de concilier bénéfices et risques.

L’OCDE rappelle aussi que les gouvernements jouent un rôle décisif dans le développement de l’infrastructure publique numérique, dont les composantes clés incluent l’identité numérique, le partage de données, les registres de base et les mécanismes de cohérence entre systèmes. Autrement dit, la littérature internationale convergente ne présente plus la circulation des données comme un enjeu périphérique ; elle la traite comme une condition de performance, de confiance et de capacité de l’État.

Au-delà des cadres institutionnels analysés, une dimension complémentaire mérite d’être explicitement prise en compte : celle des plateformes internationales de partage de données et des initiatives transnationales structurantes. Dans plusieurs domaines stratégiques, systèmes de paiement, transition climatique, biodiversité, santé ou encore divulgation des risques, des mécanismes de coordination fondés sur des normes communes et des infrastructures de données partagées sont en cours de déploiement à l’échelle internationale. Ces initiatives ne se limitent pas à des exercices de coopération technique : elles contribuent activement à la définition des normes, des protocoles et des modèles de gouvernance qui structurent les écosystèmes numériques globaux.

La capacité du Canada à participer de manière crédible à ces dynamiques repose en partie sur sa propre cohérence interne. Un cadre d’interopérabilité fédéré à l’échelle FPT ne constitue pas uniquement un levier d’efficacité domestique ; il devient également un instrument de positionnement stratégique, permettant de contribuer à l’élaboration des normes internationales et de tirer parti des apprentissages issus de ces plateformes.

Cette articulation présente un avantage opérationnel non négligeable. L’expérience montre que l’alignement sur des normes et des référentiels internationaux peut faciliter la coordination entre juridictions internes, en offrant des points d’ancrage neutres et reconnus. Elle permet également d’éviter une dépendance exclusive aux modèles externes, en positionnant le Canada non seulement comme utilisateur, mais comme contributeur actif à l’évolution des cadres internationaux.

3.9 Les conditions de succès d'un modèle fédéré

L'expérience internationale ne plaide ni pour une centralisation des données ni pour une simple collaboration ponctuelle entre administrations. Elle montre qu'un modèle fédéré peut fonctionner lorsque quatre conditions sont réunies : une orientation politique stable, des normes partagées et adaptables, des mécanismes de confiance et de conformité, et une capacité de gouvernance en mesure d'identifier, de sélectionner et de réutiliser les solutions pertinentes.

3.10 Transition vers l'opérationnalisation

Ces enseignements ne pointent pas vers un modèle unique, mais vers une architecture adaptable. C'est précisément cette architecture que la section suivante traduit en prototype opérationnel dans un contexte FPT canadien en s'appuyant sur les acquis déjà formulés dans les publications CIRANO précédentes et les développements de politiques publiques convergents.

Section 4. Du prototype conceptuel à une base opérationnelle de discussion et négociation FPT

Les transformations analysées dans les sections précédentes, qu'il s'agisse de la recomposition des infrastructures numériques, des contraintes matérielles liées à l'IA ou encore des implications croissantes en matière de sécurité nationale, convergent vers un constat commun : la capacité d'action de l'État dépend désormais de son aptitude à coordonner, à l'échelle du système, des actifs qui demeurent institutionnellement distribués.

Dans ce contexte, la formalisation d'un accord-cadre fédéral–provincial–territorial en matière d'interopérabilité des données publiques et d'adoption de l'intelligence artificielle ne relève plus uniquement d'un exercice prospectif. Elle peut désormais être envisagée comme une étape opérationnelle, rendue possible par la convergence de cadres existants, d'initiatives sectorielles et d'une volonté politique en évolution.

L'avant-projet d'accord élaboré dans les travaux préparatoires du présent document offre à cet égard une base structurée, inspirée notamment de développements récents observés au Canada et à l'international**,** tout en étant explicitement adaptée aux caractéristiques du fédéralisme canadien. Pour être utile au niveau décisionnel, ce prototype doit toutefois être lu comme une base de travail avancée, destinée à structurer une négociation intergouvernementale réelle, et non comme un texte juridique finalisé ou prescriptif. Sa valeur tient précisément à sa capacité à rendre tangibles les options disponibles, les arbitrages nécessaires et les modalités concrètes de mise en œuvre.

4.1 Une vision fédérée : rendre interopérable sans centraliser

Dans le prolongement direct de ce constat, le prototype propose une lecture renouvelée de l'interopérabilité, adaptée aux contraintes structurelles du fédéralisme canadien. Au cœur du modèle se trouve une proposition conceptuelle déterminante : l'interopérabilité ne repose ni sur la centralisation des données, ni sur leur partage généralisé, mais sur la mise en place d'un écosystème fédéré fondé sur des règles communes, des mécanismes de confiance et des capacités d'échange ciblées.

Cette distinction est essentielle dans le contexte canadien. Elle permet de concilier deux impératifs souvent perçus comme contradictoires : d'une part, la préservation des compétences et du contrôle juridictionnel sur les données, et, d'autre part, la nécessité croissante d'une collaboration intergouvernementale pour répondre à des enjeux systémiques, qu'il s'agisse de prestation de services, de sécurité nationale ou d'exploitation des capacités d'intelligence artificielle. Ainsi conçu, l'accord-cadre ne vise pas à harmoniser les systèmes existants, mais à créer les conditions de leur interopérabilité, par la définition progressive de protocoles, de normes et de mécanismes institutionnels communs, dont l'adoption demeure adaptable aux réalités des juridictions participantes. Cette approche permet d'inscrire l'interopérabilité non comme une contrainte exogène, mais comme une capacité émergente du système lui-même.

Cette approche fédérée contribue également à limiter les risques de concentration excessive et de dépendance technologique, en évitant la création de points uniques de défaillance et en maintenant une distribution des capacités entre juridictions.

4.2 Des principes structurants adaptés au fédéralisme canadien

Cette vision fédérée trouve sa traduction opérationnelle dans un ensemble de principes structurants qui encadrent l'action sans en prédéterminer les modalités. Le prototype d'accord repose ainsi sur des principes qui constituent les conditions de sa faisabilité politique et opérationnelle. Ces principes, centrage sur l'humain, le citoyen, l'utilisateur, la réutilisation des données selon le principe du « une seule fois », ouverture, sécurité, proportionnalité, responsabilité et souveraineté juridictionnelle définissent un équilibre qui se concrétise opérationnellement par des mécanismes de mutualisation encadrée entre juridictions.

Cet équilibre repose, en pratique, sur la capacité des juridictions à organiser une mise en commun ciblée de certaines fonctions, normes et mécanismes de collaboration, sans transfert de contrôle sur les données elles-mêmes.
L'un des apports les plus significatifs du modèle proposé réside dans la combinaison de trois logiques complémentaires :

- Une approche volontaire, permettant aux juridictions d'adhérer selon leurs priorités ;
- Une approche modulaire, autorisant des déploiements sectoriels ou par cas d'usage ;
- Une approche évolutive, reconnaissant la nécessité d'une transition graduelle à partir des systèmes existants.

Ce triptyque de volontariat, de modularité et de progressivité représente un levier crucial pour l'acceptabilité. Il permet d'envisager une mise en œuvre adaptable, qui prend en compte les écarts de capacités institutionnelles et les différences de priorités au sein des gouvernements. Il établit également les conditions minimales d'une collaboration soutenable dans le temps.

4.3 Une architecture de gouvernance orientée vers la collaboration et l'exécution

Sur cette base, la question de la gouvernance ne se pose plus en termes de répartition formelle des compétences, mais de capacité effective à coordonner l'action. Le prototype propose une architecture de gouvernance structurée autour d'un mécanisme de collaboration FPT chargé de soutenir l'alignement stratégique, la cohérence des approches et le suivi de la mise en œuvre. Cette structure, qui peut prendre la forme d'un conseil ou d'un forum de collaboration, est appuyée par des fonctions de secrétariat, des comités techniques spécialisés et des points de contact désignés dans chaque juridiction. Elle vise à assurer une capacité de collaboration continue, tout en demeurant adaptable aux choix organisationnels des gouvernements participants.

L’articulation envisagée avec le nouveau bureau de la transformation numérique au centre du gouvernement fédéral constitue un élément structurant, dans la mesure où elle permettrait d’arrimer les fonctions de gouvernance, de standardisation et de soutien à l’exécution, sans modifier les responsabilités propres à chaque juridiction.

Au-delà de sa configuration institutionnelle, cette architecture introduit une évolution importante : elle transforme des mécanismes de collaboration ponctuels en une capacité structurée, susceptible de soutenir une action intergouvernementale plus cohérente dans le temps, condition désormais essentielle dans un environnement marqué par l’accélération technologique. Cette architecture permet notamment d’introduire une capacité de partage des connaissances et des expériences essentielles pour anticiper les effets d’interdépendance entre systèmes et réduire les risques de propagation de défaillances à l’échelle des réseaux interconnectés.

4.4 Une innovation structurante : l’évaluation de l’interopérabilité

Dans cette perspective, la cohérence du système ne peut reposer uniquement sur des mécanismes ex post ; elle nécessite également des instruments permettant d’agir en amont. Parmi les éléments les plus structurants du prototype figure ainsi l’introduction d’un mécanisme d’évaluation de l’interopérabilité des données à valeur ajoutée, applicable aux initiatives susceptibles d’avoir un impact sur les échanges de données entre juridictions dans les secteurs stratégiques.

Inspiré notamment de pratiques internationales, ce mécanisme vise à encourager les administrations à anticiper les effets de leurs décisions, juridiques, techniques ou organisationnelles, sur la capacité d’interopérabilité entre les systèmes dans son ensemble. Il s’inscrit dans une logique de cohérence ex ante, permettant de limiter l’émergence de solutions incompatibles et de réduire les coûts associés à la fragmentation.

Au-delà de sa fonction technique, ce mécanisme constitue un instrument collaboratif puissant de gestion des risques. En favorisant l’analyse ex ante des impacts sur l’interopérabilité, il permet d’identifier en amont les vulnérabilités potentielles, les dépendances critiques et les effets systémiques susceptibles d’émerger de décisions isolées. Dans le contexte canadien, une telle approche introduite des repères communs susceptibles d’appuyer la prise de décision, tout en respectant les processus propres à chaque juridiction.

4.5 Des instruments opérationnels : expérimentation encadrée et accords d'échange

La traduction concrète de ces principes et de cette gouvernance repose toutefois sur des instruments capables de soutenir l'action au niveau opérationnel. Le cadre envisagé ne se limite donc pas à définir des orientations générales ; il prévoit des mécanismes permettant une mise en œuvre progressive et contrôlée.
Les bacs à sable d'interopérabilité permettent d'expérimenter, dans des environnements sécurisés, des solutions impliquant plusieurs juridictions, afin d'en évaluer les implications avant un déploiement plus large. Ils jouent également un rôle déterminant dans la réduction de l'incertitude, en permettant de tester les interactions entre systèmes dans des environnements contrôlés avant toute généralisation, limitant ainsi les risques d'effets non anticipés à grande échelle.

Parallèlement, les accords d'échange de données constituent des mécanismes structurants permettant de traduire les principes généraux en modalités opérationnelles adaptées à des cas d'usage spécifiques. Encadrés par des paramètres relatifs à la finalité, à la base juridique, à la sécurité, à la protection de la vie privée, et des données personnelles, à la gouvernance et à la responsabilité, ils offrent un cadre souple permettant de concilier innovation et maîtrise des risques. Cette approche permet d'opérationnaliser, à l'échelle intergouvernementale, le principe d'utilisation limitée des données, en assurant que leur réutilisation demeure encadrée, traçable et conforme aux finalités définies. Cette articulation entre expérimentation et contractualisation progressive permet de transformer des intentions en capacités concrètes, sans compromettre la maîtrise des systèmes.

Cette logique d'expérimentation encadrée trouve une application particulièrement pertinente dans les contextes nécessitant des approches adaptées aux réalités institutionnelles et culturelles. La diversité des cadres de gouvernance, des priorités et des pratiques propres aux Premières Nations rend difficile toute approche uniforme en matière d'interopérabilité des données et d'adoption de l'intelligence artificielle. Dans ce contexte, une stratégie fondée sur des projets pilotes ciblés apparaît plus appropriée qu'une intégration généralisée dès les premières phases.

Une telle approche permettrait d'expérimenter, dans des environnements définis et en collaboration étroite avec les communautés concernées, des modèles de gouvernance des données respectueux des contextes culturels, institutionnels et juridiques propres à chaque nation. Elle offrirait également un espace d'apprentissage mutuel, tant pour les administrations publiques que pour les partenaires autochtones, en vue de développer progressivement des cadres adaptés, fondés sur la confiance, la réciprocité et la reconnaissance des spécificités.

4.6 Une mise en œuvre progressive et adaptable

L'efficacité de cet ensemble dépend toutefois de sa capacité à être déployé de manière réaliste dans un environnement institutionnel complexe. Le prototype prévoit ainsi une approche de mise en œuvre fondée sur des trajectoires différenciées, tenant compte des priorités, des capacités et des contraintes propres à chaque juridiction. Cette approche peut s'appuyer sur des feuilles de route communes, des plans d'action spécifiques et des mécanismes de suivi reposant sur des indicateurs partagés, dans une perspective d'apprentissage collectif et d'amélioration continue. Des processus d'examen périodique et d'ajustement permettent d'adapter le cadre aux évolutions technologiques, organisationnelles et stratégiques, en reconnaissant que l'interopérabilité constitue un processus évolutif plutôt qu'un état final. Les mécanismes de suivi et d'amélioration continue contribuent à maintenir une capacité d'adaptation face à l'évolution des risques technologiques et organisationnels, en évitant la rigidification du système.

4.7 Garanties juridiques et respect des compétences

Cette logique de progression suppose enfin un ancrage juridique suffisamment clair pour soutenir la confiance entre les parties. L'accord intègre ainsi des garanties explicites visant à assurer sa compatibilité avec le cadre constitutionnel canadien et les régimes juridiques existants. Celles-ci participent également à la réduction des risques de perte de contrôle décisionnel, en assurant que l'augmentation des capacités d'échange et de réutilisation des données demeure compatible avec les cadres juridiques applicables et avec les exigences de confiance propres au contexte fédéral canadien.

Ces garanties s'inscrivent dans la continuité des orientations récentes du Commissariat à la protection de la vie privée du Canada, qui soulignent le rôle structurant de la protection des renseignements personnels dans le développement responsable des systèmes d'intelligence artificielle. Afin d'atteindre cet objectif, l'entente proposée établit une définition harmonisée et interopérable du terme « données anonymisées ». Cette définition s'inspire des normes de référence de facto ainsi que des pratiques réglementaires de l'OCDE et de l'UE. Selon cette définition, les données sont considérées comme anonymisées lorsque le risque de réidentification est jugé improbable en considérant le contexte dans lequel elles s'inscrivent, les technologies disponibles et les mesures de protection applicables, conformément aux cadres d'évaluation FPT convenus.

La participation des juridictions n'entraîne aucune modification de leurs compétences, et les modalités de mise en œuvre doivent être interprétées à la lumière des lois applicables, notamment en matière de protection de la vie privée, d'accès à l'information et de gestion des données. Ces garanties sont essentielles pour ancrer l'accord dans une logique de collaboration respectueuse des responsabilités de chacun, et pour soutenir une appropriation progressive par les administrations concernées.

4.8 Une base de discussion directement mobilisable pour l'action

Pris dans son ensemble, le prototype constitue une architecture fédérée et cohérente, couvrant les dimensions juridiques, techniques, organisationnelles et économiques de l'interopérabilité. Sa valeur tient à sa capacité à dépasser une approche strictement conceptuelle pour offrir une base de travail directement mobilisable dans un contexte intergouvernemental. Il permet d'engager une discussion structurée sur les modalités de mise en œuvre, tout en laissant ouvertes les options relatives au rythme, à la portée et aux mécanismes de participation.
Il s'inscrit ainsi dans le prolongement des transformations analysées dans l'ensemble du présent document : celles-ci ne pointent pas uniquement vers la nécessité d'une meilleure collaboration, mais vers l'émergence d'une capacité collective à agir de manière plus intégrée. L'architecture mise de l'avant ne constitue ni une proposition formelle ni une recommandation à ce stade. Elle vise à offrir une base de travail suffisamment structurée pour soutenir une délibération intergouvernementale informée.

Pour les sous-ministres et les décideurs, ce prototype offre un point d'appui concret pour faire évoluer les échanges actuels vers des démarches plus coordonnées, sans présumer des choix finaux qui relèveront du processus de négociation. Dans un environnement où la capacité des administrations publiques à exploiter leurs données de manière cohérente devient un facteur déterminant de leur efficacité, de leur résilience et de leur autonomie décisionnelle, un tel instrument apparaît moins comme une innovation institutionnelle que comme une réponse progressive aux exigences contemporaines de l'action publique, et comme une étape structurante vers une capacité stratégique intégrée.

Ce projet contribue également à positionner le Canada comme un acteur crédible dans les dynamiques internationales de gouvernance des données, en facilitant son alignement et sa contribution aux normes émergentes.

Conclusion

De la faisabilité à la décision : vers un mandat explicite de négociation FPT

L'analyse développée dans ce document conduit à un constat désormais difficile à contester : le Canada ne se trouve plus dans une phase d'exploration, mais à un point de bascule.
Les conditions qui rendaient, il y a encore quelques années, l'interopérabilité des données publiques difficile à envisager à l'échelle fédérale-provinciale territoriale (FPT) ne prévalent plus. Une vision stratégique de l'intelligence artificielle est en voie d'être formulée. Des usages concrets sont en déploiement dans les administrations. Un précédent institutionnel crédible en matière de coopération numérique a été établi avec l'accord FPT sur la cybersécurité de Kananaskis. Les normes, les architectures et les capacités techniques ont atteint un niveau de maturité suffisant. Autrement dit, les éléments constitutifs d'une capacité d'action mutualisée sont présents. Ce qui demeure en suspens n'est pas leur pertinence, mais leur articulation.

L'enjeu central n'est plus conceptuel. Il est décisionnel. L'absence d'un cadre structurant d'interopérabilité constitue un facteur de fragmentation qui limite la portée des investissements publics, ralentit l'adoption de l'intelligence artificielle à grande échelle et réduit la capacité des gouvernements à agir de manière cohérente face à des enjeux systémiques. Elle entraîne également une dilution des efforts, une duplication des investissements et une perte d'effet de levier collectif. Au-delà de ses implications institutionnelles, cette capacité conditionne directement la qualité des services offerts aux citoyens, la protection de leurs droits dans un environnement numérique, ainsi que leur sécurité, leur prospérité et leur qualité de vie.

À l'inverse, la mise en place d'un accord-cadre FPT permettrait de transformer une convergence encore partielle en capacité opérationnelle. Elle offrirait un mécanisme concret pour relier les initiatives existantes, orienter les investissements futurs et soutenir une montée en puissance progressive, mais structurée, de l'interopérabilité des données publiques au Canada.
Le prototype proposé dans ce document doit être lu dans cette perspective. Il ne constitue ni un modèle figé ni une proposition prescriptive. Il vise à rendre tangible une option désormais crédible : celle d'un fédéralisme opérationnel capable d'organiser la circulation sécurisée, gouvernée et utile des données, dans le plein respect des cadres juridiques applicables et des exigences de confiance propres au contexte fédéral canadien.

Sa valeur tient précisément à sa capacité à déplacer la discussion, d'un diagnostic largement partagé vers une délibération structurée sur les modalités de mise en œuvre. Dès lors, la question qui se pose aux décideurs publics devient explicite : comment organiser, dans un cadre fédéré, les conditions permettant aux données publiques de soutenir pleinement la transformation des services, l'efficacité de l'action publique et la souveraineté numérique du pays ? Répondre à cette question ne relève plus d'un exercice analytique supplémentaire. Cela implique d'engager un processus de collaboration réel, fondé sur des choix explicites en matière de gouvernance, de normes, d'incitatifs et de priorités de mise en œuvre.

L’enjeu est explicitement politique : autoriser l’ouverture d’un espace de négociation formel à l’échelle fédérale-provinciale territoriale. Une première étape concrète consisterait à confier un mandat clair aux instances compétentes, ministres responsables, sous-ministres, dirigeants principaux de l’information, afin de structurer cette transition : évaluer collectivement le prototype proposé ; identifier des cas d’usage prioritaires à fort impact ; définir un référentiel de collaboration partagé incluant des mécanismes d’expérimentation rapide, et préciser les paramètres d’un éventuel accord-cadre en matière de gouvernance, de normes et d’incitatifs.

Une telle démarche peut être engagée sans délai, dans une logique pragmatique et progressive, en s’appuyant sur les mécanismes intergouvernementaux existants. Elle ne requiert ni refonte institutionnelle ni harmonisation préalable des systèmes, mais repose sur une volonté explicite d’organiser leur interopérabilité. Ce choix n’est pas sans précédent. L’expérience récente en matière de cybersécurité a démontré que les gouvernements FPT sont en mesure d’agir collectivement lorsque les enjeux sont reconnus comme stratégiques et que les conditions de collaboration sont clairement établies.

L’interopérabilité des données constitue aujourd’hui la suite logique de cette trajectoire. Les risques associés à l’intégration des données et à l’intelligence artificielle ne sont pas minimisés. Ils constituent au contraire un élément structurant de la réflexion stratégique. Mais ces risques ne découlent pas de l’interopérabilité elle-même : ils résultent de son absence de cadre. Un système fragmenté ne réduit pas la complexité, il la déplace, la dissimule et, à terme, il la subit. Il ne limite pas les dépendances, il les subit. Il ne protège pas la capacité d’action, il l’entrave. L’enjeu n’est donc pas de ralentir la mise en relation des données stratégiques du secteur au Canada, mais de la structurer.

Le projet d’accord-cadre envisagé apporte précisément cette structuration. En introduisant des mécanismes de gouvernance, d’évaluation, d’expérimentation et de collaboration, il permet de transformer des risques diffus en variables gérables, et une complexité subie en capacité pilotée. Dans un environnement international marqué par l’accélération technologique et la recomposition des rapports de puissance, la capacité à organiser, comprendre et gouverner les systèmes de données devient un déterminant central de la souveraineté. À cet égard, l’interopérabilité encadrée ne constitue pas un risque supplémentaire. Elle constitue la condition de leur maîtrise.

L’inaction ne constitue plus une option neutre. Elle entraîne un coût croissant en inefficience, en fragmentation et en perte de capacité collective. Dès lors, la question n’est plus de savoir s’il convient d’agir, mais à quel moment et sous quelle forme cette action doit être engagée. Retarder cette étape reviendrait à prolonger une situation où les capacités existent sans être pleinement mobilisées, au coût croissant d’inefficiences systémiques et d’occasions manquées. À l’inverse, l’ouverture d’un mandat de négociation, même limité dans sa portée initiale, permettrait de structurer un espace d’action commun, d’accélérer l’apprentissage collectif et de positionner le Canada dans une trajectoire cohérente de transformation de son secteur public.

Dans un environnement où la capacité des États à mobiliser leurs données devient un déterminant central de leur performance et de leur autonomie stratégique, l'inaction comporte désormais un coût croissant, souvent invisible à court terme, mais structurant à long terme. À l'inverse, une démarche coordonnée permettrait au Canada de se doter d'un avantage comparatif durable : celui d'un système public capable de fonctionner comme un ensemble cohérent.
Le moment actuel ne garantit pas le succès d'une telle démarche. Mais il en rend la réalisation possible. L'enjeu n'est plus de produire des données, mais de les organiser pour agir collectivement, efficacement, et en temps opportun.

C'est précisément ce qui en fait un moment décisif.
Il appelle désormais une décision des gouvernements de la fédération.

Annexe, Base de travail pour un instrument FPT d'interopérabilité des données et d'adoption responsable de l'IA

Le texte qui suit présente une base de travail structurée visant à illustrer, de manière concrète, les paramètres qu'un instrument fédéral–provincial–territorial pourrait réunir afin de soutenir l'interopérabilité des données du secteur public et l'adoption responsable de l'intelligence artificielle au Canada.

Élaborée à partir des pratiques existantes en matière d'accords intergouvernementaux au Canada et éclairée par certaines évolutions récentes observées à l'international, cette base de travail propose une architecture fédérée couvrant les dimensions de gouvernance, de normes, de partage de données, de sécurité, de mise en œuvre et de suivi. Elle vise à rendre tangibles les arbitrages opérationnels, juridiques et organisationnels associés à un tel instrument, dans le respect des cadres législatifs et des compétences propres à chaque juridiction.

Cette base de travail ne constitue ni une proposition formelle ni un texte finalisé. Sa structuration volontairement avancée a pour objet de permettre une appréciation réaliste des modalités de mise en œuvre, y compris des mécanismes de collaboration, des exigences d'interopérabilité et des leviers d'incitation. Elle demeure ouverte à des ajustements, notamment en ce qui concerne le degré de contrainte, les mécanismes de financement, les dispositions d'asymétrie et les modalités d'adhésion.

Le document est présenté sous une forme proche de celle utilisée dans les accords FPT afin de faciliter son appropriation par les administrations concernées et d'appuyer, le cas échéant, des travaux exploratoires ou préparatoires. Les éléments qui y figurent peuvent être adaptés, modulés ou séquencés en fonction des priorités des gouvernements participants, incluant des approches différenciées par secteur ou par juridiction.

La lecture de cette base de travail peut se faire de manière sélective. Elle vise avant tout à offrir un point d'appui commun pour examiner, de façon informée et pragmatique, les conditions dans lesquelles une capacité interopérable à l'échelle FPT pourrait être progressivement mise en place, en cohérence avec les orientations déjà dégagées et les contraintes opérationnelles des administrations publiques. Elle est présentée à des fins de discussion et ne préjuge en rien des positions que pourraient adopter les gouvernements participants dans un cadre formel de négociation.

PRÉAMBULE

- Ce texte cherche à organiser, en vue d'une discussion, les éléments clés d'un instrument fédéral–provincial–territorial (« les Parties ») visant à favoriser l'interopérabilité des données publiques et la mise en œuvre éclairée de l'intelligence artificielle. Les parties conviennent que les données représentent un actif stratégique crucial pour assurer une prestation optimale des services publics, pour élaborer des politiques et pour renforcer la capacité d'action des gouvernements. Elles reconnaissent également que chaque juridiction possède ses propres compétences et cadres juridiques.
- Les Parties reconnaissent que l'intelligence artificielle constitue une infrastructure critique appuyant la transformation numérique du secteur public ;
- Les Parties souhaitent promouvoir un niveau élevé d'interopérabilité dans le secteur public au Canada, permettant un partage sécurisé, fiable et transparent des données ;
- Les Parties reconnaissent la répartition des compétences dans la fédération canadienne ainsi que leurs cadres juridiques respectifs, notamment en matière de protection de la vie privée et d'accès à l'information ;
- Les Parties reconnaissent les stratégies existantes en matière de données, de numérique et d'intelligence artificielle aux niveaux fédéral, provincial et territorial ;
- Les Parties reconnaissent l'importance de la confiance, de la souveraineté des données, y compris des données autochtones, et de la gouvernance responsable ;

Dans ce contexte, il apparaît utile de préciser les paramètres généraux susceptibles de structurer une telle démarche, de manière à en faciliter l'examen et, le cas échéant, l'appropriation progressive.

ARTICLE 1, OBJET ET PORTÉE

Le document établit un cadre commun visant à promouvoir l'interopérabilité des données du secteur public ; soutenir le développement de services publics numériques intergouvernementaux ; faciliter la coopération administrative, analytique et décisionnelle ; permettre le développement coordonné d'infrastructures d'intelligence artificielle ; réduire la duplication et améliorer l'efficacité et la qualité des services publics ; protéger la vie privée, la sécurité et les droits des personnes, et respecter la souveraineté des données (y compris la gouvernance des données autochtones), le cas échéant

Le mécanisme envisagé s'applique aux organismes publics participants des Parties et couvre les données personnelles et non personnelles, sous réserve des lois applicables. Il promeut le partage et la réutilisation des données et des systèmes. Il permet la mise en place de services publics numériques intergouvernementaux (par exemple, « guichet unique pour l'accès aux services des différentes juridictions. Il garantit des normes cohérentes (organisationnelles, sémantiques, techniques, juridiques) et assure la gouvernance, la responsabilité, le contrôle et la résolution des litiges. Il établit les paramètres généraux pouvant encadrer, de manière progressive et adaptable, la coopération intergouvernementale en matière d'interopérabilité des données et d'utilisation responsable de l'intelligence artificielle dans le secteur public.

La clarification de ces paramètres suppose une compréhension partagée des concepts mobilisés, afin d'assurer la cohérence des échanges et des interprétations entre juridictions.

ARTICLE 2, DÉFINITIONS

Aux fins du présent cadre, les définitions suivantes sont proposées afin de faciliter une compréhension commune des concepts mobilisés, tout en permettant leur adaptation en fonction des contextes juridiques et opérationnels propres aux juridictions participantes :

- « Organismes du secteur public », ministères, agences, institutions et organismes de statistiques qui relèvent du gouvernement fédéral, des provinces et des territoires.
- « Solution d'interopérabilité » : une spécification, une norme, une interface, un composant, un service ou une architecture qui favorise l'interopérabilité (technique, sémantique, organisationnelle et juridique).
- « Évaluation de l'interopérabilité » : évaluation formelle d'une exigence contraignante, afin d'évaluer l'impact sur l'interopérabilité.
- « Exigence structurante » : toute obligation, interdiction, condition, critère ou limite (juridique, réglementaire, technique ou organisationnelle) affectant les services publics numériques ou l'échange de données entre juridictions.
- « Bac à sable d'interopérabilité » : milieu maîtrisé favorisant le prototypage et le dépistage de solutions d'interopérabilité dans un contexte coopératif.
- « Accord d'échange de données » ou « Accord de partage de données », accord formel conclu en vertu de ce cadre pour le transfert ou le partage de données entre les parties.
- « Cadre de gestion et de gouvernance des données », politiques, rôles, responsabilités, rôles en matière de surveillance, de métadonnées, d'accès, etc.

Cet instrument applique aussi les définitions techniques incluses dans la « Recommandation du Conseil de l'OCDE sur l'amélioration de l'accès aux données et de leur partage » à laquelle le Canada adhère.

Au-delà des définitions, la mise en cohérence des approches repose sur un ensemble de principes communs susceptibles d'orienter les choix sans en prédéterminer les modalités.

ARTICLE 3, PRINCIPES

Les principes énoncés ci-après visent à orienter la mise en œuvre éventuelle d'un cadre d'interopérabilité, en fournissant des repères communs susceptibles de guider les décisions, sans préjuger des modalités spécifiques retenues par chaque juridiction.

L'interopérabilité est centrée sur l'utilisateur, favorisant le principe de collecte unique et de réutilisation des données, lorsque permis par la loi. Les solutions privilégient l'ouverture, la transparence et la réutilisation, tout en respectant les impératifs de sécurité et de confidentialité.

Les Parties collaborent à la normalisation, la qualité des données et l'utilisation de normes partagées et adaptables, tout en appliquant les principes de proportionnalité et de minimisation des données. Seules les données nécessaires à la réalisation de l'objectif doivent être partagées. La méthode la moins intrusive doit être utilisée (par exemple, la pseudonymisation, l'anonymisation lorsque cela est possible).

Chaque Partie demeure responsable de ses actions et doit assurer la traçabilité, l'auditabilité et la transparence des échanges. Les systèmes d'intelligence artificielle sont soumis à des mécanismes d'évaluation et d'approbation proportionnés. Un système d'IA audité et approuvé dans une province est soumis à une procédure accélérée pour son utilisation dans les agences fédérales, réduisant ainsi le contrôle réglementaire qui ralentit actuellement son déploiement.

L'instrument envisagé respecte la souveraineté des données et l'autonomie juridictionnelle. Les principes de souveraineté des données autochtones doivent être respectés dans les contextes pertinents. Les Parties peuvent adopter des solutions distinctes à condition d'assurer une équivalence de résultats en matière d'interopérabilité.

L'approche retenue est progressive, évolutive et fondée sur la coopération intergouvernementale. Les Parties reconnaissent que l'interopérabilité génère des gains d'efficacité pouvant être réinvestis dans la modernisation des systèmes publics. L'interopérabilité ne doit pas compromettre la protection de la vie privée ou la sécurité. Le partage des données doit être conforme à la loi sur la protection de la vie privée (fédérale), aux lois provinciales/territoriales sur la protection de la vie privée et/ou aux lois applicables. Les décisions relatives aux normes nationales et aux cadres de données sont prises par consensus.

Les parties s'engagent à coordonner la gouvernance, à résoudre les conflits et à prendre des décisions communes sur les normes, les changements, les mises à niveau, etc. La traduction de ces principes dans la pratique appelle des mécanismes de collaboration adaptés, permettant d'en assurer l'opérationnalisation dans un contexte intergouvernemental.

ARTICLE 4, GOUVERNANCE

La présente section décrit une structure de gouvernance indicative visant à soutenir la collaboration intergouvernementale, tout en laissant aux juridictions participantes la latitude nécessaire pour adapter leur participation et leurs mécanismes internes.

Un Conseil d'interopérabilité FPT est établi l'accord des Parties :

- Il est composé de représentants des gouvernements fédéral, provinciaux et territoriaux (y compris des partenaires autochtones), ainsi que d'observateurs et de conseillers techniques. Il est régi par une coprésidence permanente : l'une exercée par le gouvernement fédéral, l'autre par un représentant des provinces et territoires (désigné par rotation annuelle).
- Le Conseil constitue une instance de coordination conjointe, visant à faciliter l'alignement stratégique et la cohérence des initiatives. Il facilite et coordonne l'orientation ainsi que la mise en œuvre du cadre FPT d'interopérabilité des données du secteur public au Canada : il contribue à l'élaboration de normes consensuelles communes ; résout les litiges ; met à jour le cadre d'interopérabilité ; appuie le suivi ; coordonne le financement et l'investissement.
- Le Conseil offre aux Parties un forum fiable de partage des connaissances et des expériences pertinentes à sa mission.

- Le Conseil n'est pas un organisme consultatif. Il agit comme instance de coordination et d'alignement stratégique. Il ne dispose d'aucun pouvoir décisionnel contraignant sur les juridictions participantes, dont l'autonomie est pleinement préservée.
- Le Conseil est appuyé par un Secrétariat chargé du soutien administratif et technique ; des mécanismes partagés, des répertoires accessibles aux parties, des registres partagés, des catalogues de métadonnées, des interfaces, des portails.
- **Le Secrétariat** établit et maintient un référentiel commun des solutions interopérables, des normes approuvées, des composants réutilisables, des API, des schémas, des ontologies.

Le Bureau de la transformation numérique proposé et le Conseil fédéral-provincial territorial pour l'adoption de l'IA et l'interopérabilité des données ont des mandats complémentaires axés sur la modernisation de la prestation des services publics grâce à la technologie et aux données. Chaque organisme public participant désigne un point de contact unique chargé de coordonner les questions d'interopérabilité, d'assurer la liaison avec les autres administrations et de gérer la mise en œuvre au niveau local.

Des comités **techniques FPT** sont établis pour :

- La convergence volontaire des normes sémantiques et d'interopérabilité, de la sécurité et de la protection de la vie privée, des technologies émergentes ; l'autorisation, le suivi et l'évaluation des projets de bacs à sable d'interopérabilité et des secteurs d'activité (santé, environnement, etc.)
- Les retours d'expérience et revues conjointes de l'interopérabilité, des exigences structurantes et de leur d'un impact trans juridictionnel.

Un cadre pour une telle collaboration suppose également l'identification de composantes techniques et organisationnelles susceptibles de soutenir une convergence progressive des systèmes.

ARTICLE 5, CADRE D'INTEROPÉRABILITÉ

Les éléments présentés dans cette section illustrent les composantes possibles d'un cadre d'interopérabilité commun, incluant les normes, les outils et les mécanismes de collaboration, dans une perspective de convergence progressive et non prescriptive.

Les Parties collaborent à l'élaboration et à l'adoption progressive de normes communes couvrant les dimensions techniques, sémantiques, organisationnelles, juridiques un registre partagé des normes, solutions et composantes est maintenu.

Dans cette perspective, il devient pertinent de considérer les mécanismes permettant d'anticiper et de gérer les impacts des évolutions réglementaires et technologiques sur l'interopérabilité

ARTICLE 6, ÉVALUATIONS DE L'INTEROPÉRABILITÉ

Cette section propose un mécanisme d'évaluation destiné à soutenir la cohérence intergouvernementale des initiatives ayant un impact sur l'interopérabilité, tout en respectant les processus décisionnels propres à chaque juridiction.

Évaluations de l'interopérabilité et norme de convergence partagée

Lorsqu'une juridiction planifie une modification législative ou technique majeure (légale, réglementaire, technique ou organisationnelle) susceptible d'entraver l'échange de données interopérables ou les services publics numériques entre les juridictions (c'est-à-dire les services FPT ou multijuridictionnels), elle peut, lorsque pertinente, réaliser une évaluation de convergence.

L'évaluation prend en compte les contraintes juridiques, réglementaires et politiques ; les implications techniques et sémantiques de l'interopérabilité ; les incidences sur l'organisation, l'administration et les processus ; les incidences sur la réutilisation, les coûts et la duplication entre juridictions ; les risques pour la vie privée, la sécurité et la confidentialité ; les mesures d'atténuation possibles (alternatives, exceptions, voies de transition).

Cette évaluation peut être partagée avec le Conseil de l'interopérabilité afin de faciliter la cohérence et d'identifier d'éventuels enjeux d'interopérabilité avec les partenaires FPT. Plutôt que d'imposer une règle unique, l'évaluation propose des « passerelles d'Interopérabilité » pour maintenir le flux de données sans interférer avec l'autonomie législative de la province.

Le Conseil de l'interopérabilité peut formuler des recommandations visant à faciliter la compatibilité interopérable. Dans certaines juridictions, cela peut être lié à des évaluations d'impact réglementaire ou à des processus d'examen législatif. Les parties s'engagent à publier des résumés des évaluations (transparence), à l'exclusion des informations sensibles.
Parallèlement à ces mécanismes d'évaluation, des approches expérimentales peuvent contribuer à éclairer les choix futurs dans un cadre maîtrisé.

ARTICLE 7, BACS À SABLE D'INTEROPÉRABILITÉ

Les dispositions suivantes présentent une approche encadrée permettant d'expérimenter, de manière contrôlée et réversible, des solutions d'interopérabilité, dans le but d'éclairer les choix futurs sans créer d'obligations immédiates.

- Un bac à sable est un environnement contrôlé pour prototyper, tester et valider de nouvelles solutions d'interopérabilité (techniques, sémantiques, juridiques) impliquant une ou plusieurs juridictions sous une supervision réglementée.
- Les parties peuvent soumettre une proposition auprès du Conseil. Les critères incluent un risque minimal, des objectifs clairs, une durée définie, une stratégie de sortie, des mesures de protection de la vie privée, un plan d'impact de l'interopérabilité.
- Les projets du bac à sable font l'objet d'un suivi collaboratif et de rapports périodiques au Conseil. Lorsque des données personnelles sont impliquées, un examen par les autorités compétentes en matière de protection de la vie privée ou les organismes de surveillance est nécessaire.

- Lorsqu'une solution en bac à sable s'avère concluante, elle peut être élevée au rang de norme interopérable à part entière (après une évaluation et une approbation en bonne et due forme).
- Les participants restent responsables de leurs actes en vertu du droit applicable. L'accord doit préciser les responsabilités, les indemnisations et les recours.

Les enseignements tirés de ces expérimentations peuvent ensuite être traduits dans des modalités concrètes d'échange de données entre juridictions.

ARTICLE 8, ACCORDS D'ÉCHANGE DE DONNÉES

La présente section décrit les paramètres généraux pouvant encadrer la conclusion d'accords d'échange de données entre juridictions, en vue d'assurer la cohérence avec les principes du cadre tout en respectant les obligations légales applicables.

Dans ce cadre, lorsque deux parties ou plus échangent des données, elles peuvent conclure un accord d'échange de données (AED) (ou accord de partage de données) mettant en œuvre les principes du cadre FPT envisagé

Chaque AED précise :

- La finalité et l'utilisation, définissent la ou les raisons pour lesquelles les données peuvent être échangées ou réutilisées,
- Le champ d'application et les types de données, les éléments de données, les ensembles de données, les métadonnées.
- La base légale, le consentement, les références à l'autorité statutaire, la nécessité d'un consentement et les conditions.
- Les règles de sécurité et de protection, les normes, le cryptage, les vérifications d'accès et les enregistrements d'audit
- L'anonymisation, la pseudonymisation ou la désidentification, le cas échéant.
- Les obligations en matière de conservation, de suppression et d'archivage des données
- Les fonctions et obligations : les tâches de l'expéditeur, du destinataire, de l'administrateur, du gardien, et la gouvernance
- La qualité, normes et interopérabilité, engagements à utiliser des vocabulaires, schémas et métadonnées communs, règles de qualité
- Les responsabilité et indemnisation
- Audit, journalisation et surveillance
- La résolution des litiges/escalade
- La résiliation et stratégie de sortie
- La modification, le versionnement et la migration
- Publication/Transparence, dans les limites de la confidentialité
- Propriété intellectuelle et licences (le cas échéant)
- La gestion des incidents de sécurité et notification des violations

La mise en œuvre de telles modalités soulève également des considérations relatives au financement, aux incitatifs et à la répartition des bénéfices.
L'AED doit également respecter les régimes applicables en matière de protection de la vie privée et d'accès à l'information dans chaque juridiction. Les juridictions participantes mettent en œuvre des mesures techniques, organisationnelles et juridiques appropriées afin de soutenir et de maintenir l'anonymisation.

ARTICLE 9, FINANCEMENT ET DIVIDENDES NUMÉRIQUES

Les mécanismes présentés ci-après le sont à titre illustratif ; voici différentes approches susceptibles de soutenir la mise en œuvre d'un cadre d'interopérabilité, notamment en ce qui concerne le partage des coûts, les incitatifs et la répartition des bénéfices.

- Les Signataires reconnaissent que l'interopérabilité générera des dividendes numériques (économies d'échelle, réduction des dépenses de fonctionnement, accélération de la prestation de services).
- Le gouvernement fédéral s'engage à convertir une partie des gains d'efficience nationaux en crédits de calcul, offrant aux provinces un accès coordonné et équitable aux capacités de calcul distribuées et partagées pour leurs propres projets d'IA.
- Réinvestissement local : 40 % des économies administratives estimées selon des méthodes partagées seront directement réallouées aux juridictions participantes pour financer la modernisation de leurs systèmes hérités.

Au-delà des leviers financiers, la question centrale demeure celle des conditions pratiques de déploiement à l'échelle des administrations participantes.

ARTICLE 10, MISE EN ŒUVRE

Cette section propose des modalités de mise en œuvre graduelles, permettant aux juridictions participantes de progresser à leur rythme, en fonction de leurs priorités, de leurs capacités et de leurs contraintes opérationnelles.

- Chaque Partie élabore un plan de mise en œuvre compatible avec le référentiel de collaboration partagé comprenant les étapes, les ressources, le développement des capacités et les délais.
- Un référentiel de collaboration partagé (analogue à l'agenda européen de l'interopérabilité, pour faciliter la cohérence des investissements. Fixer les priorités et favoriser la convergence du déploiement des solutions d'interopérabilité.
- Rapports réguliers (par exemple, annuels ou semestriels) des administrations au conseil sur les progrès, les mesures et les écarts.
- Mécanismes de suivi convenus entre les parties sur l'état d'avancement de l'interopérabilité.
- Utilisation d'indicateurs communs de performance (ICP), par exemple, nombre de services interopérables mis en œuvre, nombre d'appels entre juridictions, réutilisation de composants, économies de coûts, satisfaction des utilisateurs.
- Mécanisme de retour d'expérience périodique ou revue conjointe par les pairs de la conformité aux principes, à la gouvernance et aux obligations techniques de l'accord.

- Mécanisme permettant de modifier l'accord (par exemple, par consensus ou à la majorité absolue des parties) afin de répondre aux nouvelles technologies, aux nouveaux défis ou aux nouveaux développements politiques.

Cette mise en œuvre implique notamment une gestion structurée de la transition à partir des systèmes existants

ARTICLE 11, TRANSITION DES SYSTÈMES

Les dispositions suivantes visent à encadrer la transition des systèmes existants vers des environnements interopérables, en privilégiant des approches pragmatiques fondées sur la compatibilité, la continuité et la gestion des risques.

- Accords sur la coexistence transitoire des systèmes existants, les enveloppes d'API/adaptateurs, les interfaces de transition, la conversion, la rétrocompatibilité.
- Plans d'élimination progressive des systèmes non interopérables.
- Budgétisation de la migration et du remaniement.

Dans ce cadre, certaines adaptations peuvent s'avérer nécessaires afin de tenir compte des spécificités propres à différents secteurs d'intervention.

ARTICLE 12, DISPOSITIONS SECTORIELLES

Cette section prévoit la possibilité d'adaptations sectorielles, permettant de tenir compte des spécificités propres à certains domaines d'intervention, tout en maintenant une cohérence d'ensemble.

- Le cadre d'interopérabilité envisagé peut contenir des annexes sectorielles (par exemple, santé, environnement, transport, éducation, sécurité publique) qui intègrent des normes, des règles, des vocabulaires et une gouvernance spécialisée spécifiques à un domaine.
- En ce qui concerne les données sur la santé, les initiatives FPT existantes en matière d'interopérabilité et de gestion des données sur la santé (p. ex. la Feuille de route pancanadienne partagée sur l'interopérabilité) seraient intégrées dans ce cadre,
- Pour les données autochtones, des annexes spéciales reconnaissant la souveraineté des données autochtones et les accords de gouvernance conjointe.

L'ensemble de ces éléments doit par ailleurs s'inscrire dans le respect des cadres juridiques et des obligations existantes.

ARTICLE 13, GARANTIES JURIDIQUES ET PROTECTION DE LA VIE PRIVÉE

Les éléments présentés ci-après visent à assurer la compatibilité du cadre avec les obligations juridiques existantes, notamment en matière de protection de la vie privée, d'accès à l'information et de respect des compétences constitutionnelles.

- Chaque partie doit s'assurer que sa participation et ses obligations sont conformes à ses pouvoirs constitutionnels (fédéraux-provinciaux).
- La participation n'annule pas les régimes statutaires de chaque juridiction (par exemple, la législation provinciale sur la protection de la vie privée, la loi fédérale sur la protection de la vie privée, l'accès à l'information).

- Le partage des données doit respecter les droits individuels, le contrôle, le consentement et la surveillance réglementaire.
- Lorsque des données à caractère personnel sont concernées, il existe des obligations en matière de signalement des violations, d'évaluation de l'impact sur la vie privée et de contrôle par les commissaires à la protection de la vie privée.
- En cas de flux de données entre juridictions, les règles de conflit de lois et l'harmonisation sont prises en compte.
- La protection des données sensibles ou classifiées, les exemptions et les restrictions sont clairement définies.
- Les juridictions peuvent prévoir des exceptions ou des dérogations (sous réserve de justification) dans certains domaines.

Dans ce contexte de coopération volontaire, il importe également de prévoir des mécanismes adaptés de gestion des différends.

ARTICLE 14, RÈGLEMENT DES DIFFÉRENDS

Cette section propose des mécanismes gradués de résolution des différends, inspirés des pratiques intergouvernementales existantes, et adaptés à un contexte de coopération volontaire.
Mécanisme de règlement des litiges

- Étapes : première négociation, médiation par le conseil, recours à une autorité supérieure ou à l'arbitrage.
- En cas de manquement grave, de suspension temporaire des échanges de données ou de la participation dans le but de prendre des mesures correctives.
- Responsabilité et indemnisation : recours financiers ou injonctions spécifiques.
- Sortie/Retrait : Disposition permettant à une partie de sortir de l'accord (avec préavis), et obligations transitoires pour les données et les actifs d'interopérabilité.

Ces mécanismes tiennent compte de la diversité des situations et des approches des juridictions participantes.

ARTICLE 15, ASYMÉTRIE ET FLEXIBILITÉ

Les dispositions suivantes visent à reconnaître explicitement la diversité des approches et des capacités des juridictions participantes, en permettant des modalités de mise en œuvre différenciées fondées sur le principe d'équivalence des résultats.

- Les Parties peuvent adapter la mise en œuvre selon leurs priorités.
- Toute juridiction peut adopter une solution distincte assurant une équivalence de résultats.
- Des arrangements spécifiques peuvent être établis

Enfin, la pérennité et l'adaptabilité d'un tel cadre reposent sur des modalités claires de révision et d'évolution.

ARTICLE 16, DISPOSITIONS FINALES

La présente section regroupe les modalités générales relatives à la durée, à la révision et à l'évolution éventuelle du cadre, dans une perspective d'adaptation continue.

Le cadre envisagé entre en vigueur à la signature pour une durée déterminée ; il est renouvelable.

Il peut être modifié par consentement mutuel.

Toute Partie peut s'en retirer avec préavis.

Sources et références

Gouvernement du Canada. (2026). *Un Canada fort pour tous : Mise à jour économique du printemps de 2026*. https://budget.canada.ca/update-miseajour/2026/report-rapport/pdf/update-miseajour2026-fra.pdf
Annotation.
Ce document expose la vision gouvernementale d'une « IA pour tous », structurée autour de six piliers : confiance et sécurité, développement des compétences, adoption économique, infrastructures souveraines, soutien aux champions nationaux et partenariats internationaux. Il met l'accent sur la nécessité d'une IA sécuritaire, inclusive et génératrice de prospérité. Cette source constitue un cadre stratégique de référence ; elle souligne implicitement que la réalisation de ces objectifs dépend de conditions structurantes, notamment l'interopérabilité des données et la cohérence des architectures publiques numériques.

Gouvernement du Québec. (2024). *Portrait des utilisations de l'intelligence artificielle dans l'administration publique*. https://www.quebec.ca/gouvernement/numerique/intelligence-artificielle-administration-publique/portrait
Annotation.
Ce portrait dresse un état des lieux des usages actuels de l'IA dans l'administration publique québécoise, mettant en évidence une diversité de cas d'usage sectoriels ainsi que des niveaux de maturité variables. Il illustre concrètement les opportunités d'amélioration des services publics, tout en révélant une fragmentation des initiatives et des cadres opérationnels. Cette analyse empirique renforce l'argument selon lequel l'interopérabilité des données et la structuration de la gouvernance sont des conditions nécessaires pour passer d'expérimentations ponctuelles à des gains systémiques à l'échelle gouvernementale.

Dudoit, A. (2025). *Interopérabilité fédérale-provinciale des données et adoption de l'IA : Tirer parti de la dynamique fédérale-provinciale actuelle et du partenariat stratégique Canada-UE* (2025RB-02, Rapports Bourgogne, CIRANO.) https://doi.org/10.54932/AXET1370
Annotation.
Ce rapport établit l'interopérabilité des données entre les gouvernements fédéral, provinciaux et territoriaux (FPT) comme un levier central de modernisation de l'État, de productivité et de souveraineté numérique. Il démontre que les obstacles sont principalement institutionnels et politiques plutôt que techniques. En s'appuyant sur des comparaisons internationales, notamment européennes, il propose une approche canadienne fondée sur une gouvernance fédérée et des accords modulaires. L'étude recommande la conclusion d'un accord FPT et la création d'un conseil permanent, positionné comme instruments structurants d'une transformation systémique du secteur public.

Dudoit, A., & Labillois, T. (2025). *Souveraineté numérique et fédéralisme : architecture d'interopérabilité et gouvernance de l'IA au Canada* (2025PR-11, Pour réflexion, CIRANO.) https://doi.org/10.54932/TDBZ9121
Annotation.
Cette publication conceptualise la souveraineté numérique du Canada comme reposant sur une architecture intégrée articulée autour de trois piliers : l'interopérabilité des données, les infrastructures infonuagiques souveraines et l'adoption responsable de l'intelligence artificielle. Elle met en évidence que l'absence de cadre FPT structuré limite la portée des investissements publics en transformation numérique. En s'appuyant sur des pratiques internationales, elle positionne l'interopérabilité comme une infrastructure essentielle nécessitant harmonisation des normes, mutualisation des capacités et mise en place d'une gouvernance FPT permanente.

Dudoit, A., Labillois, T., & Oliveira, C. (2026). *Interopérabilité des données du secteur public au Canada et adoption responsable de l'IA : Synthèse stratégique et appel à l'action* (2026PR-01, Pour réflexion, CIRANO.) https://doi.org/10.54932/VOKC1489

Annotation.

Ce document constitue un appel à l'action politique structuré autour de trois impératifs : amélioration de la productivité publique, renforcement de la souveraineté numérique et adoption responsable de l'intelligence artificielle. Il met en lumière le décalage entre une collaboration FPT opérationnelle existante, mais fragmentée et l'absence de cadre politique pérenne. L'interopérabilité y est définie comme une infrastructure stratégique nationale. Le rapport préconise la mise en place d'une gouvernance FPT durable, portée au plus haut niveau politique, assortie d'un échéancier de mise en œuvre crédible.

Dudoit, A. (2026). *Souveraineté numérique et intelligence artificielle au Canada : De la fragmentation des systèmes à la capacité stratégique intégrée du secteur public* (2026PR-04, Pour réflexion, CIRANO.) https://doi.org/10.54932/AFQN6960

Annotation.

Cette étude approfondit la transformation numérique en intégrant sa dimension matérielle et géoéconomique, soulignant que l'intelligence artificielle repose désormais sur des infrastructures physiques critiques, notamment énergétiques et de données. Elle élargit l'analyse à une approche FPT+ incluant les municipalités et les Premières Nations. L'interopérabilité y est présentée comme un levier central pour structurer un marché intérieur intégré et résilient. Le rapport propose une feuille de route opérationnelle (2026–2028) combinant gouvernance, cas d'usage stratégiques et renforcement des capacités institutionnelles.

Union européenne, Référence structurante

Commission européenne. (s. d.). *Interoperable Europe Portal*.
https://interoperable-europe.ec.europa.eu/

Annotation.

Portail central de mise en œuvre de l'interopérabilité à l'échelle européenne : Il documente les outils, standards, cas d'usage et mécanismes de collaboration entre États membres.
Cette référence offre une preuve concrète d'opérationnalisation à grande échelle et montre que l'interopérabilité est un écosystème vivant, pas un cadre théorique. Elle illustre les bacs à sable, solutions réutilisables, communautés de pratique.

Commission européenne. (s. d.). *Interoperable Europe Board*
https://interoperable-europe.ec.europa.eu/collection/governance-board

Annotation.

Instance de gouvernance réunissant États membres et Commission : Elle coordonne les orientations stratégiques en matière d'interopérabilité. Cette référence offre un exemple concret de mécanisme FPT structuré et démonte l'argument selon lequel une gouvernance fédérée serait irréaliste.

Union européenne. (2024).
Règlement (UE) 2024/903 du Parlement européen et du Conseil du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union (Règlement pour une Europe interopérable*)*
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R0903
Annotation.
Cadre juridique contraignant établissant une obligation d'interopérabilité dans le secteur public européen : une référence normative forte pour cette étude ; justifie l'introduction de mécanismes comme les évaluations ex ante et les obligations de cohérence. Cette référence positionne le prototype comme moins contraignant et bien adapté à la réalité canadienne.

Australie, Modèle opérationnel intégré

Australian Government. (2023). *Data and Digital Government Strategy*.
https://www.dataanddigital.gov.au/strategy
Annotation.
Stratégie intégrée liant données, numérique, services et expérience citoyenne.
Cette référence confirme que l'interopérabilité est un levier de transformation globale et renforce l'approche systémique (pas sectorielle)

Australian Government. (s. d.). *Secure data exchange*.
https://architecture.digital.gov.au/capability/secure-data-exchange
Annotation.
Cadre technique et organisationnel pour l'échange sécurisé de données. Cette référence donne du contenu concret à la notion de confiance et de sécurité opérationnelle.

Australian Government. (s. d.). *Application programming interfaces (APIs)*.
https://api.gov.au/
Annotation.
Cette référence positionne les API comme infrastructure clé de l'interopérabilité et appuie l'argument selon l'interopérabilité repose sur des

Australian Government. (2023). *Protecting Australians*.
https://www.digital.gov.au/strategy/data-and-digital-government-strategy/protecting-australians
Annotation.
Lien explicite entre données, sécurité et confiance publique.

AI Plan for the Australian Public Service 2025 (s. d.).
https://www.digital.gov.au/policy/ai/australian-public-service-ai-plan-2025
https://www.digital.gov.au/policy/artificial-intelligence/ai-plan-australian-public-service
Annotation.
Plan concret d'intégration de l'IA dans l'administration publique. Cette référence montre que l'IA est déjà institutionnalisée ailleurs et renforce l'urgence pour le secteur public au Canada.

Australian Government. (2023). *What we heard*.
https://www.dataanddigital.gov.au/strategy/about-strategy/what-we-heard
Annotation.
Cette référence résume les résultats de consultations publiques en Australie et fait ressortir que les juridictions demandent elles-mêmes plus de partage de données, tout comme c'est le cas dans l'UE

OCDE, Cadre conceptuel international
OECD. (2019). *Enhancing access to and sharing of data*.
https://doi.org/10.1787/276aaca8-en
Annotation.
Ce rapport analyse des bénéfices et risques du partage de données et fournit une base analytique solide pour l'arbitrage risques/bénéfices ainsi que la gouvernance

OECD. (2024). Digital public infrastructure for digital governments
Annotation.
https://www.oecd.org/digital/digital-public-infrastructure/
Annotation.
Positionne les données, l'identité numérique et les registres comme infrastructures publiques essentielles. Les données = infrastructure stratégique