CIRANO

Knowledge into action

DIGITAL SOVEREIGNTY AND FEDERALISM: DATA INTEROPERABILITY AND AI GOVERNANCE

ALAIN DUDOIT
TONY LABILLOIS

PR

2025PR-12
FOR REFLECTION

The papers For Reflection... aim to propose, through applied research results or discussion documents, actions to be taken to accelerate recovery, ensure sustainable economic growth, energize Quebec's regions and reduce the future budget deficit while maintaining adequate funding for health and education. These documents are the sole responsibility of the authors.

Les documents Pour Réflexion... visent à proposer, par l'entremise de résultats de recherche appliquée ou de documents de réflexion, des actions à privilégier pour accélérer la reprise, assurer une croissance économique durable, dynamiser les régions du Québec et résorber le déficit budgétaire à venir tout en maintenant un financement adéquat pour la santé et l'éducation. Ces documents sont sous la seule responsabilité des auteurs.

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.

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 Partners - *Les partenaires du CIRANO*

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

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

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. *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.*

ISSN 2563-7266 (online version)

Digital Sovereignty and federalism: Data Interoperability and AI governance

Alain Dudoit
Ambassador of Canada (ret.)
CIRANO Invited Fellow
Strategic Advisor, Global Advantage Consulting Group

Tony Labillois
Consultant in accessibility, public policy, leadership, and data
Retired Director General at Statistics Canada
Elected Member of the International Statistical Institute

2 décembre 2025

Pour citer ce document / To quote this document

Dudoit, A., & Labillois, T. (2025). Digital Sovereignty and federalism: Data Interoperability and AI governance (2025PR-12, Pour réflexion, CIRANO.) https://doi.org/10.54932/DNAN8237

Table of contents

Summary

Canada is at a strategic inflection point. Its digital sovereignty depends directly on three inseparable levers: data interoperability across federal, provincial and territorial (FPT) governments; sovereign cloud infrastructure; and the responsible adoption of artificial intelligence (AI) in the public sector. These levers form an integrated architecture that drives productivity, digital security, government modernization and the country's capacity to address the current fragmentation of public information systems.

Analysis of the 2025 federal budget confirms an ambitious repositioning around productivity, economic sovereignty, infrastructure resilience and digital transformation. However, in the absence of an explicit FPT framework for data interoperability, investments remain dispersed and struggle to produce systemic effects. Canada nonetheless has structural advantages: a tradition of intergovernmental collaboration an internationally respected national statistical system and a proven ability to build shared governance mechanisms. Today's fragmentation, spread across fourteen heterogeneous digital infrastructures with divergent standards, metadata and identifiers, directly undermines public-sector efficiency, critical-infrastructure security and the responsible use of AI.

The CIRANO Burgundy Report (CIRANO, 2025) underscores that the Canadian federation has the conceptual foundations to build federated data governance, provided the legislative framework is modernized (including an update to Bill C-27), institutional responsibilities are clarified, and mutualization of resources approaches are strengthened.
International comparisons, particularly with the European Union, show that jurisdictions that have successfully advanced digital transformation rely on robust interoperability architectures, common repositories, standardized trust frameworks and mechanisms for pooling digital capabilities.

Technical considerations demonstrate concretely what is required: harmonized metadata, common identifiers, secure sharing mechanisms, sovereign cloud infrastructures and compatible modular services. Recent steps—the creation of the Office of Digital Transformation (ODT), investments announced in Budget 2025 and the emerging vision for a sovereign cloud, are significant but insufficient without a structured FPT framework for public-sector data interoperability and AI adoption.

This analysis highlights that data interoperability must be recognized as essential infrastructure, on par with energy networks and transportation corridors. It is indispensable for consistent public services, lower transaction costs, stronger privacy protection, crisis resilience and value creation through AI. The identification of high-value FPT data, risk management, digital operational sovereignty and the role of shared entities reinforce the need for a permanent FPT Board on data interoperability and AI.

By harmonizing standards, investments and institutional capacities, FPT governments can transform current digital fragmentation into a driver of cohesion, productivity, sovereignty and public innovation. FPT interoperability and responsible AI are not technical add-ons; they are the foundations of a strong, sustainable and truly sovereign Canadian digital economy.

Budget 2025: Building a Strong Canada[iii]

Budget 2025 establishes the fiscal and institutional conditions for a fundamental restructuring of Canada's public-sector and economic architecture.
International evidence indicates that countries linking public-sector AI initiatives to data interoperability and sovereign infrastructure accelerate service efficiency and industrial competitiveness.

The OECD's analysis[iii]of the EU's coordinated AI plan (2025) illustrates how multi-level governance can ensure coherence. The European Union has coordinated AI strategies across 27 Member States by setting common objectives, combining investments and establishing shared mechanisms and common data-governance standards.
For Canada, the EU experience demonstrates that jurisdictional diversity can be an asset when effective coordination mechanisms are in place. A Canadian counterpart to the European Interoperability Committee would enable federal, provincial and territorial actors to collectively manage standards, ethics, data and AI-enabled service delivery.

Converging analyses—including the OECD report and CIRANO's work[iv], lead to a single conclusion: Canada cannot successfully execute the proposed digital transformation without FPT data interoperability and coordinated AI governance. These are not incidental technical projects; they are essential tools for public-sector productivity, economic prosperity and intergovernmental and social cohesion.

Budget 2025 appears to recognize this structural challenge but addresses it primarily through budget consolidation and workforce reduction. The creation of the Office of Digital Transformation (ODT) is a step forward, but its mandate remains federal rather than federated or federative. The opportunity lies in redefining digital transformation as a shared capacity between the federal government and the provinces and territories, rather than as a purely federal reform.

To take the next step, however, several elements must be modernized and harmonized: FPT legislative frameworks for the protection of personal information; digital infrastructure enabling secure real-time exchanges; and common standards for metadata, identifiers and sectoral classifications.
These principles should be integrated into the modernization programme led by the new ODT. Mandated to lead the adoption of AI and emerging digital technologies across the federal government, the ODT will play a central role in aligning digital initiatives.

It will contribute directly to the productivity and transformation objectives set out in Budget 2025, including the commitment to build a leaner and more efficient public service.
The ambitions of Budget 2025 can only be achieved if the public sector at the federal, provincial and territorial levels is able to keep pace. While fiscal measures provide new levers for transformation, business diversification and national integration, success will depend on the ability of the federal government and its partners to harmonize AI-driven transformation and data interoperability across jurisdictions and sectors.
Just as railways, highways and energy networks enabled Canada's development, interoperable data must be recognized as essential shared infrastructure. It enables secure, citizen- and business-centred services, drives economic competitiveness through AI innovation and ensures resilience in times of crisis.

1. Industrial strategy, productivity and the domestic market

Budget 2025 signals a clear commitment to accelerate the modernization of Canada's productive capital after a decade of underinvestment.

Two fiscal levers dominate: the super-deduction for productivity and the reintroduction of the Accelerated Capital Cost Allowance. These measures encourage equipment renewal and primarily target SMEs.

The government is also investing in emerging technologies: AI, quantum computing, life sciences and clean energy. These investments are substantial but remain fragmented. Canada continues to struggle to convert research niches into durable economic advantages. The industrial strategy is progressing but does not yet fully articulate the path linking innovation, productivity and the consolidation of local ecosystems.
The Budget reaffirms the importance of accelerating the adoption of emerging technologies, strengthening competitiveness through private investment and protecting critical supply chains in key sectors.

2. Procurement policy and economic sovereignty

The budget marks a strategic shift toward Made-in-Canada procurement. Public purchasing is positioned as a lever to support domestic businesses, secure supply chains and encourage local innovation. Several measures—including the creation of the Major Projects Office and investments in sovereign digital infrastructure—reinforce this orientation.
This strategy could be more explicit. Stronger support for Canadian cloud providers and advanced technology manufacturing firms would further the goal of digital and industrial sovereignty.

3. Artificial intelligence, digital sovereignty and critical infrastructure

Artificial intelligence plays a central role in Budget 2025, presented as a driver of economic and public-sector transformation. The government reaffirms its aim to unlock the potential of AI in the public sector and highlights digital sovereignty, including reduced dependence on foreign infrastructure.
Funding for a sovereign cloud—$925.6 million over five years, with initial announcements in 2024—represents a major milestone. This infrastructure targets sectors handling highly sensitive data such as health, public finance, critical infrastructure and government services.
The Canadian Infrastructure Bank's mandate has been expanded to include AI infrastructure, confirming a public—private co-investment strategy for essential platforms.
Several departments—Shared Services Canada, Justice and Transport—are expanding the use of AI. The TechStat programme will analyze AI use, risks and socio-economic impacts.
Observers note that limited support for domestic cloud providers and the absence of a robust data-governance framework weaken the impact of these investments.

4. Modernization of the State

Transforming the federal government is a pillar of the Budget. The government plans to reduce the size of the public service, streamline internal services and restructure to generate $60 billion in savings over five years.
This modernization relies on automation, digital technologies and AI to improve administrative efficiency.
The strategy raises a capacity challenge: staff reductions coincide with rising demand for digital skills. The public service must do more with less while maintaining strong, competent governance.
A credible digital transformation depends on internal capacity to understand, govern and operate systems. As the federal framework and the CIRANO Burgundy Report emphasize, technology strategies—AI, cybersecurity or service transformation—cannot deliver results if organizations lack the skills to implement and oversee them.
Investment is essential in data science, information architecture, platform engineering and AI governance, supported by managerial capacity to lead complex digital transformations. Specialized career paths, accessible continuing education and structured partnerships with Canadian universities and public centres of expertise should be part of a sustained effort to reduce external dependency and enable the government to fully assume its digital responsibilities.

5. FPT collaboration and data interoperability

Budget 2025 implicitly recognizes the need to improve FPT coordination—through modernized digital infrastructure, controlled establishment of service platforms, investments in a sovereign cloud and strategic harmonization of major projects via the Major Projects Office.

Canada does not yet have a formal FPT framework for data interoperability, limiting the effectiveness of several budget initiatives. Without an explicit framework, integrated projects in areas such as health, mobility and energy risk remaining fragmented. Budget 2025 reinforces the urgency of a modernized legislative framework, notably through the update and relaunch of Bill C-27 on responsible AI and data governance.

Several initiatives—TechStat, cloud reform and AI infrastructure—would be more effective if accompanied by an FPT agreement on data governance, akin to the European Union's approach to data interoperability.

This gap underscores the relevance of the recommendations in the Bourgogne Report.

6. International dimension and Canada's positioning

Viewed internationally, Budget 2025 aligns Canada with partners such as the G7, the European Union and Australia on digital sovereignty, responsible AI, critical infrastructure, value-chain security and government modernization.

Unlike these partners, Canada lacks a structured FPT mechanism for data and technology governance. FPT interoperability—as proposed in the Bourgogne Report—should be the structuring element enabling Canada to operationalize its international ambitions.

This international dimension warrants sustained attention in any discussion of data interoperability and AI adoption in the Canadian public sector.

Alignment with the G7: Investments in sovereign cloud and critical infrastructure strengthen digital sovereignty. TechStat and renewed work on C-27 align with the G7's approach to trustworthy AI.

Convergence with the European Union: The Interoperable Europe Act and the EU AI Act create consistent frameworks for public interoperability. Canada could further harmonize standards.

Parallel with Australia: Australia illustrates that digital transformation requires an explicit data-sharing framework and consistent national standards.

Exposure to American dynamics: Canada remains dependent on U.S. cloud and AI providers. The Budget seeks to reduce this dependence but stops short of a Canadian-cloud-first policy.

7. Legislative framework: Bill C-27[v] and data governance

The Budget does not propose direct measures regarding Bill C-27 but underscores the urgency of strengthening it to support digital trust, data governance and responsible AI.

The government has signalled its intention to resume consideration of the bill. Substantial updates are essential before reintroduction. Canada's patchwork of privacy laws, access-to-information regimes and data-sharing rules poses major obstacles to the secure, responsible flow of data.

Operational interoperability requires accelerated harmonization of FPT frameworks: clarified responsibilities, standardized definitions, agile authorization mechanisms and harmonized models for data sharing and acquisition. Regulatory consistency would accelerate exchanges between administrations and strengthen public confidence by ensuring a uniform level of protection and transparency across Canada.

Strategic measures adopted by the government—and elements of the Budget—digital sovereignty, adoption of AI in the public sector, new critical infrastructure and administrative modernization—require a modern, clear and operational legal framework covering data protection; high-risk systems; algorithmic transparency; management of sovereign cloud infrastructure; interoperability of high-value public-sector datasets; and shared responsibilities for data governance.

To ensure that the proposed framework for public-sector data interoperability and AI adoption preserves privacy and is future-proof, three families of advanced techniques—differential privacy, secure multi-party computation and federated learning—should be deployed, based on use cases, to enable high-value analyses without sharing raw data.

These approaches require standardized governance, common toolkits and consistent privacy and threat-risk assessments across jurisdictions. At the infrastructure level, a sovereign FPT cloud should adopt a zero-trust security posture; enforce encryption and enclave-based processing; ensure Canadian residency and custody of data and cryptographic keys; and incorporate Indigenous data governance protocols. Together, these measures provide a technically credible foundation for secure, high-impact collaboration between governments while strengthening public trust, regulatory compliance and long-term resilience.

8. Implications for interoperability and public AI

Three observations stand out: digital sovereignty requires FPT interoperability; public AI requires standardized data; and Canada should draw on European and Australian models. Budget 2025 creates levers but not yet the architecture. This is the role of the proposed FPT agreement on public-sector data interoperability and AI adoption.
Budget 2025 proposes an ambitious path forward, but success depends on a clear FPT implementation framework, increased support for domestic suppliers and strengthened shared governance of high-value data in the public sector.

The public sector can play a leading role in Canada's responsible digital transformation, with AI at its core. This lever is grounded in exclusive legislative and regulatory responsibilities, the public sector's weight in the economy, the breadth of programmes and services and extensive data assets covering Canadian realities at home and abroad.

> "Reaping the benefits of AI while mitigating the threats it poses will not automatically follow from the technology itself and its current siloed development. It will require a concerted effort to implement adjustments and controls in institutions, regulations and technologies. Governments are best placed to play a leading role in this coordinated effort." (Haddad et al., 2025).

The challenge of sovereignty in the digital age

Digital sovereignty emphasizes the autonomy of Canada's data ecosystem, infrastructure and intellectual property for the public good. Sovereignty is defined as Canada's capacity to shape its digital destiny while balancing national autonomy and international cooperation. True sovereignty requires legal applicability in Canada, not solely physical data location.
Digital sovereignty, interoperability and trust are mutually reinforcing pillars. Canada's future digital governance must combine legal applicability, infrastructure interoperability and inclusive governance.

The global shift toward secure, ethical and sovereign data systems underscores the need for governments to act together as strategic stewards of their digital assets. In Canada, the division of responsibilities among federal, provincial and territorial governments creates structural asymmetries that hinder coordinated, consistent implementation. Digital sovereignty is now central to Canada's economic and institutional future.

The challenge is not only infrastructure but governance: how to harmonize data, technology, policy and regulatory systems across FPT jurisdictions while protecting constitutional autonomy.
Recent economic visions of the federal government and Quebec converge on this point: both regard digital modernization as essential to productivity, security and digital sovereignty.

Digital sovereignty in the face of intergovernmental reality

Digital sovereignty cannot be achieved without secure, robust infrastructure capable of supporting essential services. The federal framework emphasizes resilience, continuity and availability—attributes that depend on the quality of the underlying infrastructure. This includes modernizing public data centres, diversifying cloud models, managing digital identities in a sovereign manner and implementing integrated data architectures based on common standards.

An FPT strategy for sovereign digital infrastructure would reduce risks associated with dependence on international suppliers, strengthen cybersecurity and ensure that critical public data—and the tools needed to maximize its benefits—remain under Canadian control. Such a strategy should include systemic resilience mechanisms, such as distributed redundancy and FPT digital crisis-management protocols.

Strengthening data interoperability must go hand in hand with developing national large-scale computing capacity.

As highlighted by the Digital Research Alliance of Canada (2025), sovereignty in AI depends on both data governance and the mastery of sovereign computing. Without a national AI backbone—a publicly administered supercomputer comparable to international infrastructures—Canada will remain dependent on foreign hyperscalers, limiting its ability to develop, train and govern domestic AI models. Integrating sovereign computing capacity into an FPT data-interoperability architecture is a necessary condition for complete digital sovereignty.

At the heart of public governance are citizens—taxpayers, consumers, workers, entrepreneurs—and end users of services. Interoperability directly addresses frustrations with duplication, delays and inefficiency.

Citizens and businesses are entitled to complementary, efficient, secure and reliable services. Interoperability is the backbone that enables this. For businesses, harmonized data standards reduce compliance costs and create a level playing field across jurisdictions.

The dual functionality of citizen-centred FPT data interoperability and its mission

<table>
<tr><td colspan="2">Safeguarding democracy
• Transparency and accountability: open, evidence-based decision-making
• Equity and inclusion: detection of disparities and guarantees of fairness
• Resistance to misinformation: authorized and timely communications
• Political legitimacy: public trust in public institutions
• National resilience and operational effectiveness</td></tr>
<tr><th>Direct users (ministers, MPs, senior civil servants)</th><th>End users (citizens, businesses, taxpayers)</th></tr>
<tr><td>• Evidence-based decisions—consistent and comparable data across federal, provincial, and territorial governments
• Forward planning and risk management AI-based analyses, scenario modelling
• Crisis response—faster and more coordinated action across jurisdictions
• Strategic capacity—clearer long-term planning based on solid data
• Stronger intergovernmental alignment: common vocabulary, shared governance, synchronized decisions.
• Reduced administrative friction: fewer manual exchanges, less duplication.</td><td>• Continuous services: complementary interactions, independent of jurisdictions.
• Efficiency: reduction of duplication and acceleration of processing.
• Personalization: AI anticipates needs and adapts services.
• Economic value: harmonization of compliance reduces costs for businesses.
• AI quality, security, and transparency</td></tr>
</table>

The federal—provincial—territorial context: from fragmented systems to shared capacity

Canada's FPT digital-governance ecosystem is marked by institutional fragmentation. Federal departments maintain diverse data infrastructures, while provinces and territories operate their own frameworks and standards. This fragmentation hinders efficiency and scalability in the public service, particularly for AI deployment and evidence-based decision-making.

Fragmented and siloed data systems lead to duplication, delays and costly failures. Citizens and businesses expect seamless, secure and efficient services, which governments cannot deliver without interoperable databases. AI requires reliable, high-quality, up-to-date and interoperable data to support responsible, agile public decision-making.

Canada has a solid foundation in its national statistical system on which to build federated interoperability for public-sector data and AI adoption. Statistics Canada has long demonstrated that jurisdictional diversity can be reconciled with operational consistency. Existing FPT mechanisms, joint committees, common technical standards and bilateral data-sharing agreements have enabled a federated architecture that respects provincial and territorial jurisdictions. This experience shows that Canada already has a collaborative model, professionally independent structures and a networked approach that foreshadows the governance required for system interoperability and responsible AI.

Establishing an FPT Board on Data Interoperability and AI Adoption in Canada's public sector (see appendix) is necessary for prosperity and public well-being. This formal joint governance mechanism would include provinces, territories, Indigenous governments and municipalities. It would oversee standards, data quality, AI ethics and digital security. By strengthening human capacity, advanced cybersecurity and quantum preparedness, Canada can adapt the European model of coordinated AI and data governance to its federal reality.

Such development is not a break with the past; it extends FPT cooperation that already works and can serve as the foundation for truly shared capacity in Canada's public sector.

In the EU model, resources mutualization (pooling) refers to sharing technical, legal and organizational capacities among Member States and EU institutions to collectively address public issues that transcend borders. Pooling is based on three mechanisms: (1) common standards—data, classifications, technical interoperability and security—that allow each state to connect to the common system without losing sovereignty; (2) shared platforms and infrastructure (e.g., data spaces, exchange points, digital identities) that reduce costs and promote secure flows; and (3) joint governance—Member States retain internal powers but collectively delegate standards definition, risk oversight and operational coordination to a common body:

- The Interoperable Europe Committee recommends interoperability solutions for the cross-border interoperability of networks and information systems used to provide or manage public services that must be provided or managed electronically in the Union. When an interoperability solution is recommended by the Interoperable Europe Committee, it is labelled an "Interoperable Europe solution" and published on the Interoperable Europe portal.

This model creates a shared capacity set of harmonized, interconnected resources that enables each Member State to act more effectively than alone, while maintaining decision-making autonomy. Mutualization is not a transfer of powers; it is a structured alignment of resources to achieve collective results otherwise impossible.

While EU law offers a compelling reference, Canada's context differs. The EU can legislate binding interoperability standards, enforced by centralized institutions. Canada operates under a federal constitutional architecture in which provinces and territories hold exclusive jurisdiction over many data-generating sectors (health, education, justice, and natural resources).

Federal action in Canada must be based on collaborative federalism: co-creation of standards, voluntary adoption, bilateral and multilateral agreements and sustained policy alignment.

Progress may be slower, but solutions are better tailored to local realities. Canada must build an interoperability ecosystem grounded in negotiated governance, shared infrastructure, common incentives and trust-based partnerships—including Indigenous governments, whose data jurisdictions further differentiate the Canadian landscape.

European-style pooling is compatible with Canadian federalism. It does not transfer constitutional powers; it creates common standards and capabilities for voluntary adoption. It respects existing divisions of responsibility while providing a common framework for data, digital security and AI.
Canada has implemented functional pooling mechanisms in Statistics Canada, the Canadian Food Inspection Agency, Public Safety, Environment and Climate Change Canada, joint registries and FPT epidemiological surveillance systems.

Sharing digital resources in Canada's public sector does not centralize federal powers. It establishes a flexible national framework that can be supplemented by FPT agreements, as European regimes are by Member State commitments. Bill C-27 is not an obstacle to pooling; it provides a foundation, provided an intergovernmental agreement clarifies shared responsibilities, common standards and joint governance.

Four federal initiatives in context

These four recent federal initiatives will shape Canada's digital-governance landscape: the 2025–2027 AI Strategy for the Federal Public Service, the Digital Sovereignty Framework, the Sovereign Cloud Initiative and the AI Strategy Working Group.
These four initiatives are summarized in this table

Initiative	Main scope	Institutional objective	Governance gaps
AI Strategy for the Federal Public Service (2025–2027)	Responsible use of AI in federal departments	GC employees, AI knowledge, governance, and infrastructure	Encourages FPT collaboration, the AI economic ecosystem or Indigenous frameworks.
Digital sovereignty framework (2025)	GC data and digital infrastructure as an institution	Internal preparation and legal management of protected data B	Excludes Indigenous data sovereignty, intergovernmental collaboration, and the broader economy.
Sovereign Cloud Initiative (Major Projects Office (MPO/DFAIT)	Secure cloud computing and computing infrastructure controlled by Canada	Advanced computing and AI/quantum ecosystems	FPT and industry participation unclear
AI Strategy Working Group (2025–2026)	Next-generation AI policy through consultations	Government-wide and public engagement approach	Exploratory, not yet institutionalized

These initiatives aim to strengthen Canada's digital readiness. They operate at different levels—governance, infrastructure and engagement—and remain largely federal in scope. Differences in scope create a governance gap that could fragment sovereignty efforts: strong at the centre, weak at the periphery.
Canada's digital reforms are ambitious but risk perpetuating fragmented data spaces if not anchored in a federated interoperability framework at the heart of the new national AI strategy.

Success requires clear intent to engage all levels of government and an ambitious, realistic plan developed with stakeholders and supported by necessary resources.

1. The AI Strategy for the Federal Public Service (2025–2027) emphasizes responsible adoption within the federal government.

The new AI Strategy for the Federal Public Service (2025–2027) highlights collaboration: "We are collaborating on the adoption of AI with Indigenous and Canadian partners, other Canadian and international governments, and our colleagues in the public service." However, it excludes adoption by organizations outside the Government of Canada.

This strategy and its predecessors—the 2018 Data Strategy Roadmap and the 2023–2026 Federal Public Service Data Strategy—emphasize data sharing and collaboration across levels of government but do not propose detailed measures specifically addressing interoperability between federal and provincial public services.

2. Federal Digital Sovereignty Framework (2025): scope, limitations and complementarity with an FPT interoperability framework.

The federal government's digital sovereignty framework defines autonomy as the ability to protect, manage and control Government of Canada systems and data, regardless of supplier or infrastructure location. Sovereignty extends beyond data residency to operational resilience, system integrity, cloud risk management and institutional control. The framework sets out an architecture for data residency, vendor risk assessment, encryption, digital identity and compliance.

Canada's dependence on foreign digital infrastructure—particularly U.S. infrastructure—exposes the country to interference, extraterritorial surveillance and geopolitical vulnerability. In this context, the federal framework provides an essential foundation for institutional protection, economic support and national security.

Its strictly federal scope, however, limits systemic impact. It does not extend to vast data ecosystems managed by provinces and territories, which are critical to health, energy, the environment, employment, social services, internal trade and major risk and disaster management—pillars of national resilience and public AI training. Nor does it incorporate Indigenous data governance, which is essential for legitimacy, trust and equity. The framework is not contradictory to an FPT interoperability framework; it is complementary.

The federal framework establishes minimum standards for security, data governance and risk management that can serve as a common foundation. An FPT framework—as described in the Burgundy Report—would extend standards across the federation, harmonize intergovernmental technical standards, integrate Indigenous governance and link public data management to national economic objectives.

Indigenous Data Sovereignty (IDS) should be treated as a structural requirement of any credible FPT interoperability and AI framework. Indigenous nations have constitutional rights, and their data—territorial, environmental, demographic, cultural and community-generated—are integral to programmes, infrastructure planning and land and resource management. A national architecture that does not fully integrate IDS principles risks reinforcing colonial administrative models.

Implementing IDS requires integrating established governance frameworks—OCAP®, CARE and EGAP—into FPT data and AI systems. This includes codeveloped data-sharing agreements; community-defined access and consent protocols; Indigenous representation in governance bodies; and mechanisms recognizing Indigenous stewardship through metadata, access controls and audit trails. Semantic interoperability should reflect Indigenous knowledge systems, languages and classifications to avoid imposing colonial taxonomies on community data.

IDS also has implications for responsible AI adoption. Indigenous governments should be directly involved in AI risk assessments, particularly where algorithmic decisions have significant impacts, and communities must retain control over training datasets involving Indigenous data. Integrating IDS strengthens national data systems by improving completeness, legitimacy and reliability while fostering innovation in land management, climate resilience and community health.

3. The Sovereign Cloud Initiative[vi] aims to establish a secure national infrastructure for critical systems.

In September 2025, the Prime Minister asked the Major Projects Office to develop a Canadian sovereign cloud—a national digital infrastructure to secure data, expand computing capacity and support competitiveness.

The sovereign cloud is intended to be the cornerstone of digital sovereignty, ensuring that Canada controls infrastructure hosting sensitive public data and advanced research, alongside tools to maximize economic, social and security benefits, within an appropriate legislative and regulatory framework.

While the initiative is in the early stages, its inclusion in MPO priorities reflects a fundamental policy shift: digital infrastructure is a strategic nation-building project on par with pipelines, ports and nuclear projects.

Sovereignty alone does not guarantee interoperability. The sovereign cloud must explicitly incorporate interoperability protocols, metadata standards and federated identity tools and systems.

Its relevance to FPT data governance is immediate and significant. Integrating common standards and shared tools into a sovereign cloud would provide a secure basis for inter-administrative data exchange, enabling provinces, territories and municipalities to share information securely and efficiently.

4. The new national AI strategy[vii] must promote the interoperability of FPT public-sector data and intergovernmental harmonization of AI deployment in the public sector.

In the coming months, the government is expected to present a renewed national AI strategy. This strategy should integrate the initiatives described above and ensure coherence. It must make FPT data interoperability a central pillar—not a technical upgrade, but a vital national infrastructure, akin to railways, energy networks or universal health care.

Canada can no longer afford fourteen siloed digital infrastructures across FPT jurisdictions; inefficiencies and costs are too high. Citizens, businesses and decision-makers must be able to distinguish truth from misinformation, and the risks to digital sovereignty are too great to delay.

Conclusion—From sovereignty to cohesion: building a unique, strong and sustainable Canadian digital economy and society

Canada is at a strategic turning point. Digital sovereignty cannot be achieved through isolated federal programmes or ad hoc reforms. It requires a coherent, federated architecture for data governance and AI adoption. By harmonising investments, standards and governance across jurisdictions, Canada can transform its digital fragmentation into a driver of cohesion and competitiveness.

Canada faces an unprecedented convergence of pressures on its innovation ecosystem.
The latest report from the Council of Canadian Academies (CCA) (18 November 2025) — The State of Science, Technology and Innovation in Canada in 2025 — provides one of the clearest and most urgent assessments of the country's declining innovation capacity in more than a decade.
Its findings reinforce and amplify the central argument of the CIRANO report: federal, provincial, and territorial data interoperability and the accelerated and reliable adoption of AI are no longer optional improvements to public administration, but structural prerequisites for Canada's economic resilience, social cohesion, and international competitiveness.
The evidence presented by the CCA is unambiguous. Canada's productivity crisis continues to worsen, technology adoption is lagging in most sectors; business R&D intensity remains chronically low; and our fragmented innovation policy framework is not keeping pace with global technological and geopolitical changes. The panel concludes that without systemic, coordinated and ambitious action, Canada risks a lasting erosion of its standard of living, institutional capacity and national competitiveness.
The CCA report [7]also highlights the need for coordinated governance. Canada's innovation ecosystem remains fragmented across jurisdictions and sectors, weakening the country's ability to mobilise its national strengths. This validates CIRANO's call for a permanent FPT governance body to oversee interoperability standards, data management and the responsible deployment of AI, i.e., an institutional pillar capable of harmonising policies, investments and regulatory approaches.

AI is identified by the CCA as a transformative, versatile technology, but its adoption remains uneven and social trust fragile. High-quality, interoperable data is essential for building reliable, verifiable and context-appropriate AI systems. Without clear data traceability, shared standards and common taxonomies, Canada cannot develop responsible AI in the public or private sectors.

The CCA also highlights a significant ‘data deficit’ in Canada's innovation system: existing measures are outdated and do not reflect modern data-driven dynamics. An interoperable data ecosystem between the federal, provincial and territorial levels would greatly improve real-time monitoring, evaluation and forecasting, enabling more adaptive and evidence-based innovation policy.

Internationally, the Council of Canadian Academies (CCA) highlights the importance of partnerships with like-minded countries. CIRANO's focus on aligning Canadian interoperability efforts with new Canada-EU digital frameworks positions Canada to participate in trusted data spaces, cross-border AI governance, and transatlantic innovation value chains. Domestic reforms and international alignment are mutually reinforcing.
Canada is reaching a tipping point where digital sovereignty, economic competitiveness, and federal cohesion depend directly on its ability to establish a coordinated framework for data interoperability and responsible AI governance.
Converging analyses by CIRANO and the Council of Canadian Academies show that the current architecture—composed of fourteen disjointed FPT digital infrastructures, an incomplete legislative framework, and federal initiatives limited to their own scope—cannot support either the digital transformation of the public sector or Canada's ambitions for productivity, security, and sovereignty.

Yet the country has unique structural assets: an exemplary national statistical system, a long tradition of intergovernmental collaboration, and a potential for pooling resources comparable to that of the most advanced European models.

Now is the time to transform this solid foundation into a shared FPT capacity: joint governance based on common standards, interoperable infrastructure, and a consistent update of the legislative framework, including a modernised C-27. The establishment of a permanent FPT Council on data interoperability and AI, supported by national data asset mapping, would be the decisive institutional tool to ensure policy consistency, investment transparency, infrastructure security and public confidence.
The issue is no longer technical: it is strategic. It is a national construction project. By acting now, Canada can convert its current digital fragmentation into a driver of cohesion, innovation and sovereignty — and finally build a strong, sustainable and forward-looking Canadian digital economy and society.

Digital sovereignty cannot be bought; it must be built! Just as railways, highways and energy networks have enabled Canada's economic and social development, interoperable data must be recognized as essential shared infrastructure: it must be treated as such by the Major Projects Office. It enables secure, citizen-centred services, stimulates economic competitiveness through AI innovation and ensures resilience in times of crisis. This common infrastructure will enable the delivery of major projects that will transform and connect the Canadian economy.

Canada does not yet have any global digital champions. It will only assert credible and sustainable digital sovereignty by combining ambitious regulation, massive investment, sovereign innovation, coordinated FPT action, and talent development. To create dynamic ecosystems for the development of cutting-edge AI, it will be necessary to mobilise computing resources, data, and talent. Canada must invest in research and critical infrastructure, such as sovereign cloud, networks, semiconductors, quantum computing and data gigafactories.

Recommendations

To ensure sustainable digital sovereignty, Canada must act simultaneously on two inseparable pillars: FPT interoperability of public-sector data and a national sovereign computing capacity for AI. Five priorities emerge:

1. Treat public-sector data interoperability and sovereign computing as essential infrastructure—planned and funded as national strategic assets.
2. Establish an integrated data—computing—AI strategy, supported by national mapping of high-value public-sector data to guide investment and secure AI uses.
3. Conclude a formal FPT framework for data and AI governance through an FPT Board on public-sector data interoperability and AI adoption.
4. Deploy a national AI backbone based on a public supercomputer administered by an independent FPT organization.
5. Strengthen public-sector capacity and institutional readiness through training, talent development and modernization to reduce dependency on external providers.
   A coherent digital state requires a competent civil service capable of managing complex data ecosystems, overseeing digital platforms, ensuring cybersecurity, and governing AI systems responsibly. Investments in training, talent development, and institutional modernization are essential to build long-term capacity and reduce dependence on external providers.

By leveraging these five levers, Canada can transform current digital fragmentation into a coherent, resilient and sovereign ecosystem capable of supporting public innovation, productivity and national security. Digital sovereignty cannot be built into isolation; interdependencies require active international cooperation with trusted partners such as the European Union, which shares a focus on fundamental rights, infrastructure security and responsible AI governance.

Background

The proposed framework for FPT data interoperability and responsible AI adoption

The CIRANO Burgundy Report (2025RB-02) provides a practical roadmap for strengthening Canada's federated digital capacity and identifies five priority actions:

Action 1	**Comprehensive mapping of FPT high value datasets** • Identify datasets in priority sectors • Assess governance & gaps • Build sector-specific roadmaps
Action 2	**FPT data interoperability agreement** • Flexible, opt-in model • Defines roles, standards, governance • High-value datasets prioritized • Supports modernization & collaboration
Action 3	**FPT AI & data interoperability board** • Evolves from current informal annual symposium • Mandate: strategy, oversight, dispute resolution • Aligns with Office of Digital Transformation • Promotes open, practical solutions
Action 4	**Economic incentives for participation** • Federal co-investments in cloud, cybersecurity, AI hubs • Encourages trust, participation, and capacity building
Action 5	**Deepening Canada–EU digital partnership** • Builds on Canada–EU Digital & Strategic Partnership • Leverages EU experience (Interoperable Europe Act) • Priorities: AI, digital identity, privacy, interoperability • Enhances sovereignty & resilience

Each measure advances interoperability without undermining provincial, territorial or Indigenous sovereignty. For Quebec—which prioritizes efficiency and performance—this model aligns with its Economic Vision 2025. The report's logic is pragmatic: governance, collaboration and recognition of data as a national strategic asset—rather than technology alone—are the cornerstones of digital sovereignty.

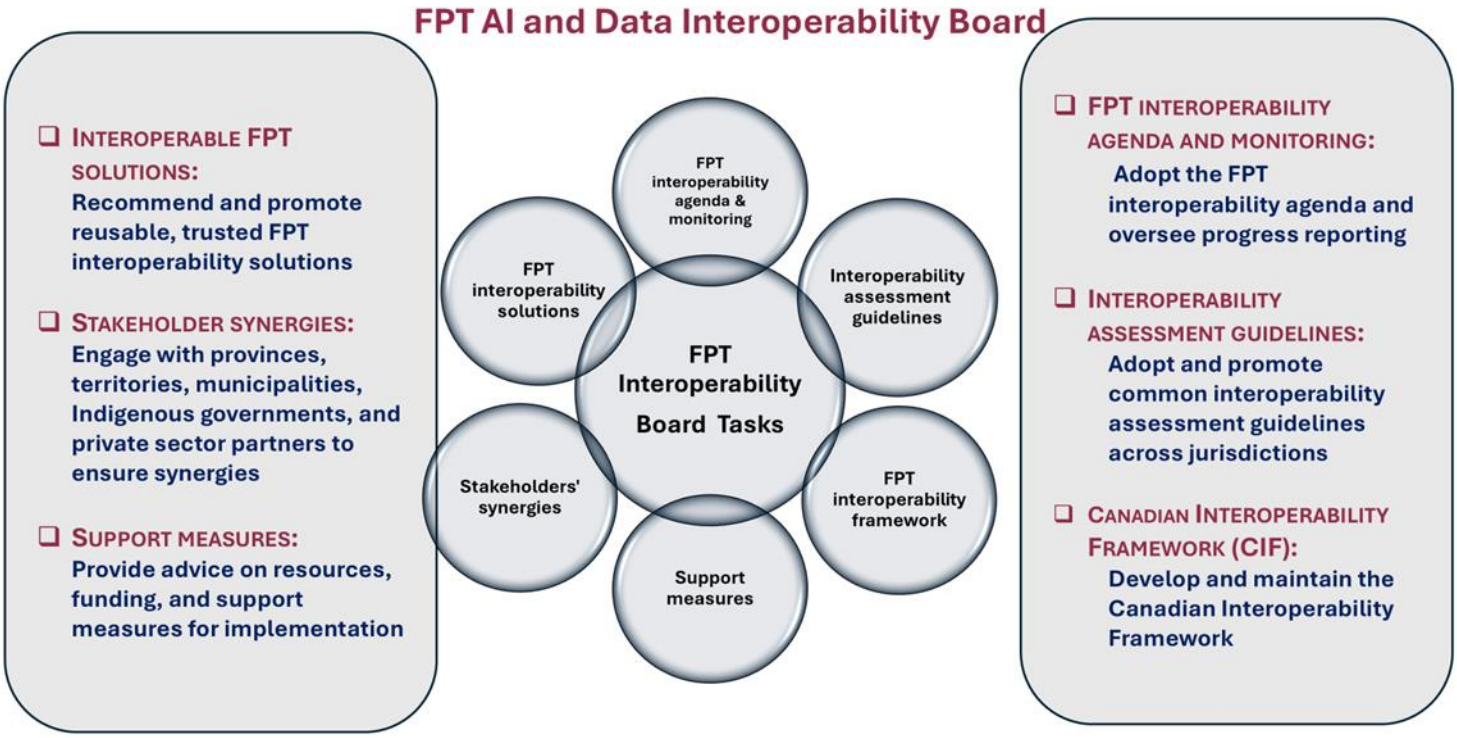
The first stage of FPT mapping will establish the factual basis (datasets, standards and digital assets) needed for effective implementation of the ODT mandate, while the proposed FPT Council will provide the governance and evaluation framework required for financial accountability and interjurisdictional learning.

Mapping high-value data assets is fundamental to interoperability. It promotes transparency, identifies redundancies and reveals opportunities for efficiency through AI. The FPT mapping initiative proposed in the CIRANO Burgundy Report—jointly led by the Treasury Board Secretariat CIO/ODT and the Privy Council Office—offers a low-risk, high-return mechanism for harmonizing jurisdictions.

This mapping will also support future co-investments in AI, cybersecurity and the development of data infrastructure. By identifying shared datasets in energy, health, community protection and mobility, governments can prioritize phased transformation funding where added value is greatest.
The CIRANO Burgundy Report proposes a concrete governance framework to implement Canada's digital sovereignty through collaboration, not centralization.

The opportunity for an FPT Board on data interoperability and AI adoption in Canada's public sector

A permanent FPT governance mechanism is essential to ensure measurable progress in a coherent, responsible and ethical transformation of Canada's public sector. The proposed federated board on AI and data interoperability would be co-chaired by the Privy Council Office (Intergovernmental Affairs) and the Treasury Board Secretariat (Office of the Chief Information Officer), with support from Statistics Canada and relevant counterparts from participating provinces and territories:



Such a board would strengthen trust among FPT partners and institutionalize data governance as a central element of Canada's economic and security architecture. Integrating OECD-style performance indicators would ensure transparency and measurable results.

- ***Institutionalizing FPT coordination transforms ad hoc collaboration into a sustainable governance model for digital sovereignty.***

Technical considerations for FPT data interoperability and responsible AI adoption

This appendix summarizes key technical considerations that complement the five actions proposed in the CIRANO Burgundy report. These considerations do not prescribe a single technical approach; they identify feasible paths toward a unified, standards-compliant plan aligned with international benchmarks and Canada's distinctive leadership characteristics.

1. Basic metadata standards

A common metadata foundation enables discovery, exchange and reuse of data across jurisdictions. A pragmatic national foundation can be based on a layered standards model:

• DCAT/DCAT-AP (with a Canadian profile)—suitable for general government datasets and API catalogues, aligned with OECD and EU interoperability frameworks; a Canadian DCAT profile would standardize dataset descriptions, access conditions and API endpoints across FPT organizations.

• ISO 19115/19139 for geospatial data—widely used by FPT GIS programmes, ensuring consistency of geolocated data for environmental management, emergency response and infrastructure planning.

• SDMX (Statistical Data and Metadata eXchange)—an ISO standard for describing statistical data and metadata, standardizing exchange and improving efficient sharing among statistical organizations.

2. Advancing semantic interoperability

Semantic alignment requires technical tools and coordinated governance.

Bilingual terminology—Canada should establish a machine-readable terminology and ontology service providing controlled vocabularies in English and French. Existing resources such as TERMIUM Plus, Statistics Canada classification systems and GC Digital Exchange vocabularies can serve as a foundation.

Indigenous Data Sovereignty—Semantic models should incorporate Indigenous governance principles (OCAP®, CARE, EGAP), with dedicated metadata elements capturing governance, management and authorizations; codeveloped ontologies and vocabularies; and mechanisms for community-specific access rules in data-sharing agreements.

Domain-specific ontologies—Sectors such as health, environment and justice may require alignment with international ontologies (e.g., SNOMED CT, INSPIRE) while preserving Canadian-specific terminology and bilingual equivalencies.

3. Role of the GC Enterprise Architecture (EA)

The GC EA provides an institutional platform to ensure consistency and interoperability at scale through:

• Reference architectures and mandatory interface standards for federal systems, with recommended models for provincial/territorial harmonization.

• Processes for evaluating, validating and updating technical standards (metadata, APIs, security controls) based on performance and evolving best practices.

• Master plans for shared services—identity and credential management, consent management, data-exchange gateways and AI model lifecycle management—reusable by partners to reduce implementation costs and timelines.

Technical considerations for data sharing that preserve the confidentiality and security of the sovereign cloud

This appendix provides a concise overview of the technical elements necessary to implement privacy-preserving data sharing in an FPT framework for public sector data interoperability and responsible AI adoption. It also describes the recommended security posture for a sovereign cloud designed to support sensitive intergovernmental data exchanges. These elements complement the policy analysis presented in the main report and respond to expert comments received during the review process.

1. Implementation of privacy-preserving data sharing techniques

A modernized FPT framework must enable secure, high-value analysis while maintaining strong privacy protections. Three categories of techniques—differential privacy (DP), secure multi-party computation (SMPC) and federated learning (FL)—offer complementary pathways.

Alignment of use cases:

• Differential privacy (DP) is effective for statistical outputs, dashboards and public publications where disclosure risks must be limited. Applying DP requires defining and managing privacy budgets and documenting use cases where reduced accuracy is acceptable.

• Secure multi-party computation (SMPC) supports joint computation among jurisdictions that cannot exchange raw data (e.g., health, justice, revenue datasets), delivering exact or near-exact results while preventing exposure.

• Federated learning (FL) enables distributed model training among custodians who retain control over local records; FL should be combined with secure aggregation and/or DP to mitigate model-extraction and inversion risks.

Operational requirements:

• Classify use cases by sensitivity, legal constraints and required outcomes.

• Use a standardized decision matrix to match use cases with appropriate privacy techniques.

• Employ hybrid architectures (e.g., FL+DP for training or SMPC+DP for secure publication).

• Develop reusable FPT toolkits and test beds for rapid prototyping and evaluation.

• Institute robust governance, including privacy and threat-risk assessments, data-sharing agreements with algorithmic controls and independent validation of DP or cryptographic implementations.

2. Security posture for a sovereign FPT cloud

A sovereign cloud supporting interoperable exchanges and advanced analytics must incorporate a verifiable security and governance architecture compliant with Canadian legal, regulatory and sovereignty requirements.

Fundamental security principles:

• Zero-trust architecture with continuous authentication, least privilege and micro-segmentation of workloads.

• Encryption at rest and in transit, supported by Canadian-controlled key management, including options for customer-managed or shared-custody keys.

• Trusted execution environments (TEEs) enabling enclave processing of sensitive analytical and cryptographic protocols.

• Immutable, tamper-evident audit logging supporting traceability, forensic readiness and transparent reporting to FPT data owners.

• Data residency and jurisdictional assurance ensuring sensitive datasets and cryptographic material remain in Canada.

• Supply-chain security, including secure built pipelines, software bill of materials (SBOMs) and third-party audit requirements.

Governance considerations:

• Multi-level data zoning aligned with provincial and Indigenous classifications.

• Enforcement of Indigenous data-governance frameworks, including OCAP® and CARE, through technical controls (e.g., access restrictions, consent logs and verifiable traceability).

• Independent certification, including ITSG-33 alignment and industry standards such as ISO 27,001, SOC 2 and CSA CCM.

This security posture ensures that interjurisdictional data flows can occur with confidence, while respecting legal obligations, cultural protocols, and public expectations.

3. Recommended next steps

In order to embed these technical principles into practice, three initial actions are recommended for the proposed FPT Council on Data Interoperability and AI Adoption in the Canadian Public Sector:

1. Create an FPT working group on privacy and security, with Indigenous representation, to define risk tolerances, privacy budgets and sovereignty requirements.

2. Develop an interoperability and assurance guide mapping data types to appropriate privacy techniques and cloud-sovereignty controls.
3. Launch one or two interjurisdictional pilot projects leveraging privacy-preserving methods in a sovereign-cloud test bed to validate feasibility and inform scaling decisions.

Comparison table: EU vs. Canada—Implications for AI interoperability and governance

Dimension	European Union (supranational model)	Canada (federal constitutional model)
Legal authority/constitutional basis	Supranational legal order: EU regulations (e.g., the AIE) are binding on all Member States.	Division of powers in the Constitution Act; provinces/territories have jurisdiction over key areas of the public sector. No federal authority has the power to impose interoperability standards across all sectors.
Governance structure	Centralized coordination through the European Commission, the European Interoperability Committee and cross-border digital working groups.	Collaborative federalism: governance through FPT councils, bilateral agreements, memoranda of understanding, ministerial tables and jointly developed frameworks.
Policy instruments/legal levers	EU regulations, delegated acts, binding technical standards, and harmonized data frameworks.	Policy frameworks, funding agreements, common standards, procurement levers, federal-provincial agreements; voluntary adoption.
Institutional capacity	Strong supranational institutions (DG DIGIT, interoperable Europe) are capable of defining and enforcing interoperability standards.	The institutional landscape is divided between federal ministries, provinces, territories, and Indigenous governments. No central enforcement body.
Incentives for adoption	Compliance enforced through binding regulations and access to EU funding/programmes.	Incentives based on co-funding, infrastructure sharing, performance frameworks, and alignment with national priorities (e.g., productivity, service improvement).
Rapid and uniform implementation	Faster and more uniform implementation thanks to a centralized authority and binding standards.	Slower and more variable implementation across jurisdictions due to differing priorities, capacities, and political cycles.
Jurisdiction over Indigenous/minority data	EU Member States retain their national responsibilities; indigenous data sovereignty is not a fundamental structural issue.	Indigenous governments have inherent jurisdiction over data; principles of reconciliation and data sovereignty require dedicated governance models and joint design.
Interoperability infrastructure	Cross-border digital services, European data spaces, common data models, and interoperable digital public goods imposed at the EU level.	Federated digital infrastructure evolving through FPT cooperation; requires negotiated standards, shared registries, common data platforms, and trust frameworks.

Acronyms and abbreviations

Acronym/Concept	English Definition	Definition en Français
DCAT/DCAT-AP (Canadian profile)	Standard for describing datasets to make them discoverable and shareable. DCAT-AP is the EU adaptation; The Canadian profile ensures FPT and Indigenous datasets are compatible.	Norme pour décrire les ensembles de données afin de faciliter leur découverte et partage. DCAT-AP est l'adaptation européenne ; le profil canadien assure la compatibilité des données fédérales, provinciales, territoriales et autochtones.
DP	Differential Privacy: A technique that adds statistical noise to data or results in order to protect individuals' identities and sensitive information, while still allowing useful analyses to be conducted.	Confidentialité différentielle : Technique qui ajoute du bruit statistique aux données ou aux résultats afin de protéger l'identité et les informations sensibles des individus, tout en permettant des analyses utiles.
SMPC	Secure Multi-party Computation: A cryptographic method that allows multiple parties to collaborate to perform a calculation on their combined data without ever revealing their respective data.	Calcul multipartite sécurisé : Méthode cryptographique permettant à plusieurs parties de collaborer pour effectuer un calcul sur leurs données combinées sans jamais révéler leurs données respectives.
FL	Federated Learning: A machine learning approach where models are trained directly on local devices or servers, without centralizing data. Only the model parameters (not the raw data) are shared.	Apprentissage fédéré : Approche d'apprentissage automatique où les modèles sont entraînés directement sur les appareils ou les serveurs locaux, sans centraliser les données. Seuls les paramètres du modèle (et non les données brutes) sont partagés.
API (Application Programming Interface)	Standard way for software systems to communicate and exchange data.	Méthode standard permettant aux systèmes logiciels de communiquer et d'échanger des données.
GIS Programmes (Geographic Information Systems)	Tools to capture, analyze, and visualize location-based data for planning and decision-making.	Outils pour capturer, analyser et visualiser des données géolocalisées pour la planification et la prise de décisions.
TERMIUM Plus	Canada's official terminology database for standardized French and English usage.	Base de données officielle du Canada pour une terminologie uniforme en français et en anglais.
OCAP®, CARE, EGAP	Indigenous data governance principles: OCAP® (Ownership, Control, Access, Possession), CARE (Collective Benefit, Authority, Responsibility, Ethics), EGAP (Engage, Govern, Access, Protect).	Principes de gouvernance des données autochtones : OCAP® (Propriété, Contrôle, Accès, Possession), CARE (Bénéfice collectif, Autorité, Responsabilité, Éthique), EGAP (Engager, Gouverner, Accéder, Protéger).
GC EA (Government of Canada Enterprise Architecture)	Blueprint for designing and connecting government IT systems, promoting interoperability.	Schéma directeur pour concevoir et interconnecter les systèmes informatiques gouvernementaux, favorisant l'interopérabilité.

Zero Trust Baseline	Cybersecurity approach assuming no user or device is trusted by default; every access must be verified.	Approche de cybersécurité où aucun utilisateur ou appareil n'est de confiance par défaut ; chaque accès doit être vérifié.
TLS 1.3	Encryption protocol for secure data transmission over networks.	Protocole de chiffrement pour sécuriser la transmission des données sur les réseaux.
OIDC/SAML with RBAC/ABAC	Identity standards (OIDC/SAML) for secure login; RBAC (role-based) and ABAC (attribute-based) control access.	Normes d'identification (OIDC/SAML) pour une connexion sécurisée ; RBAC (contrôle basé sur les rôles) et ABAC (contrôle basé sur les attributs) pour gérer l'accès.
Tamper-Evident Logging	Logging methods that prevent undetected modification: WORM/blockchain, centralized SIEM, role-based log access.	Méthodes de journalisation empêchant toute modification non détectée : WORM/chaîne de blocs, SIEM centralisé, accès aux journaux selon les rôles.
SBOMs (Software Bills of Materials)	List of all components in software to identify vulnerabilities and ensure security.	Liste de tous les composants d'un logiciel pour détecter les vulnérabilités et assurer la sécurité.
ISO 27001, CSA CCM, SOC 2, ITSG-33/TBS Guidance	Standards for IT and cloud security: ISO 27 001 (global), CSA CCM (cloud), SOC 2 (audit), ITSG-33/TBS (Canada).	Normes de sécurité informatique et infonuagique : ISO 27 001 (internationale), CSA CCM (cloud), SOC 2 (audit), ITSG-33/TBS (Canada).
• **ISO 19,115** • **ISO 19,139**	• Geospatial metadata content • XML format for representing this metadata	• Contenu des métadonnées géospatiales • Format XML pour représenter ces métadonnées
SLAs (Service Level Agreements)	Agreements defining expected performance, uptime, and support of IT systems.	Ententes définissant la performance attendue, la disponibilité et le soutien des systèmes informatiques.

Acronym/Concept	Definition in French	Definition in French
TEE	Trusted Execution Environment: Secure execution environment within a processor. Allows code to be executed and data to be processed without interference from the operating system, applications, or attackers.	Environnement d'exécution sécurisé au sein d'un processeur. Permet d'exécuter du code et de traiter des données à l'abri du système d'exploitation, des applications et des attaquants.
ITSG-33	**IT Security Risk Management (Canada)** Standard of the Communications Security Establishment (CSE) of Canada. It provides a framework for managing information security risks for Government of Canada systems.	Norme du Centre de la sécurité des télécommunications (CST) du Canada. Elle fournit un cadre de gestion des risques de sécurité de l'information pour les systèmes du gouvernement du Canada.
ISO 27,001	**Information Security Management System (ISMS)**	Norme internationale définissant les exigences pour mettre en place un système de gestion de la sécurité de l'information.
SOC 2	**Service Organization Control Type 2** The audit report conducted by an independent third party in accordance with AICPA guidelines. Evaluates a service provider's internal controls based on five principles: security; availability; processing integrity; confidentiality; privacy protection.	Rapport d'audit effectué par un tiers indépendant selon le cadre de l'AICPA. Évalue les contrôles internes d'un fournisseur de services selon cinq principes : sécurité ; disponibilité ; intégrité du traitement ; confidentialité et protection de la vie privée
AICPA	**American Institute of Certified Public Accountants.**	Organisme professionnel national des comptables agréés (CPA) aux États-Unis. Il établit plusieurs normes reconnues internationalement, dont celles qui encadrent les audits SOC 1, SOC 2 et SOC 3.
CSA CCM	**Cloud Controls Matrix** Cloud Security Alliance (CSA) standard. This is a framework of best practices and security controls for the cloud.	Standard de la Cloud Security Alliance (CSA). Il s'agit d'un cadre de bonnes pratiques et de contrôles de sécurité pour le nuage

Sources and references

[1] A Strong Canada Budget 2025 https://budget.canada.ca/2025/report-rapport/pdf/budget-de-2025.pdf

[2] OECD; Progress in Implementing the European Union Coordinated Plan on Artificial Intelligence (Volume 1) Member States' Actions—https://doi.org/10.1787/533c355d-en

[3] Dudoit, A. (2025). Federal-Provincial Data Interoperability and AI Adoption: Leveraging Current Federal-Provincial Momentum and the Canada-EU Strategic Partnership (2025RB-02, Burgundy Reports, CIRANO.) https://doi.org/10.54932/AXET1370

[4] Legislative summary of Bill C-27: An Act to enact the Consumer Privacy Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts. Publication No. 44- 1-C27-E PDF 1.12 MB, (46 Pages) 022-07-12

[5] Matt Swayne. Carney Pushes for Sovereign Cloud as Canada Navigates Quantum Future Quantum Insider. 12 September 2025: https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as- canada-navigates-quantum-future/

[6] Innovation, Science and Economic Development Canada: Government of Canada launches Task Force on Artificial Intelligence Strategy and public consultation to develop Canada's next AI strategy

[7] CAC — Council of Canadian Academies, 2025. The State of Science, Technology and Innovation in Canada 2025, Ottawa, ON, Expert Panel on the State of Science, Technology and Innovation in Canada, CAC. https://doi.org/10.60870/fabx-mp29