DENTONS

Clarifying the law on digital and AI sovereignty

May 2026

As the race for AI development and adoption accelerates, claims for data sovereignty and concerns about extraterritorial legal reach rise.[1] The pursuit of digital sovereignty is rightfully put in doubt[2] while it has also become "the watchword driving Canada's digital policy agenda."[3] The statement by the Treasury Board of Canada Secretariat that "it is impossible for the GC to obtain a state of complete digital sovereignty … due to the absolute interconnected nature of the digital world,"[4] applies to both government and business. Yet, the necessity for both states and industry to protect their data remains critical. We examine here the law applicable to digital and AI sovereignty to identify the legal measures available to block or, more realistically, manage foreign access to data.

The push for digital sovereignty is global in view of the risk created by the convergence of AI's powerful data outputs and the centralization of AI development in a few companies and countries. In the European Union (EU), France and Germany have made European digital sovereignty an element of their Franco-German Economic Agenda, including a summit on European digital sovereignty.[5] The private sector is also engaged, notably through Jolt Capital V, which announced a first closing of €600 million to finance European deep tech companies in fields including semiconductors, applied artificial intelligence and technical software.[6] In the UK, the government has launched a £500 million Sovereign AI initiative to back homegrown AI companies.[7] Japan's allocation of US$9.9 billion toward chip research and development, plus US$3.1 billion for domestic advanced chip production, reflects the same policy direction.[8] China's pursuit of "cyber sovereignty," positing cyberspace sovereignty as an extension of national sovereignty, is well established.[9]

On December 17, 2025, the Government of Canada announced the signing of a memorandum of understanding (MOU) with Coveo Solutions Inc., a Québec-based Canadian applied-AI company specializing in AI-search and AI-relevance technology. Under the MOU, Coveo will assist Shared Services Canada (SSC) and Innovation, Science and Economic Development Canada (ISED) in exploring "the deployment of Canadian-developed, AI-powered enterprise solutions across the Government of Canada." This agreement implements the government's commitment in Budget 2025: *Canada Strong* to procure "made-in-Canada sovereign AI tools for the public service." The objective is AI sovereignty, with Coveo providing local technological capacity as part of the Government of Canada's sovereign AI procurement strategy.[10]

Digital and AI sovereignty is not merely a matter of investments, capacity building or policy direction. It is also a matter of law, dictating technological specifications, corporate governance structures and protective contractual measures. It engages public international law (defining state sovereignty), conflict of laws rules (governing the exercise of national jurisdiction) and privacy law (regulating cross-border data flows).

For governments, data sovereignty means preserving decision-making power over their data and protecting it from extraterritorial access. For businesses, data sovereignty rules determine their rights and obligations when facing foreign government access requests. Our objective here is to identify the legal requirements of digital and AI sovereignty and the legal measures available to assert it.

1. For purposes of this article, "data sovereignty" refers to legal and operational control over access to data, including foreign-state access; "digital sovereignty" refers more broadly to control over digital infrastructure and capabilities; and "AI sovereignty" refers to the legal, operational and technological capacity to develop, deploy and govern AI systems and related data. Jurisdiction-specific statutory terms such as "personal data," "personal information," and "bulk US sensitive personal data" are used where the applicable legal regime requires them.
2. Joshua Van Es, Can Canada ever have true digital sovereignty? Globe and Mail, March 25, 2026
3. Michael Geist, The catch-22 of Canadian digital sovereignty, Globe and Mail, December 10, 2025.
4. Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada.
5. *Franco-German Economic Agenda*, ÉLYSÉE (September 1, 2025), https://www.elysee.fr/en/emmanuel-macron/2025/09/01/franco-german-economic-agenda.
6. *First closing of Jolt Capital V at €600m*, JOLT CAPITAL (Nov. 27, 2025), https://www.jolt-capital.com/news/first-closing-of-jolt-capital-v-at-600m.
7. *AI firms pioneering drug discovery, cheaper supercomputing and more get first backing through UK's Sovereign AI*, GOV.UK (Apr. 16, 2026), https://www.gov.uk/government/news/ai-firms-pioneering-drug-discovery-cheaper-supercomputing-and-more-get-first-backing-through-uks-sovereign-ai.
8. Japan Earmarks Extra $9.9 Billion for Chips and AI This Year, Bloomberg
9. *Sovereignty in Cyberspace: Theory and Practice (Version 2.0)*, CYBERSPACE ADMIN. OF CHINA (Nov. 25, 2020), https://www.cac.gov.cn/2020-11/25/c_1607869925296336.htm.
10. La Presse, Coveo aura la tâche de moderniser l'appareil fédéral, December 17, 2025

1. The notion of "sovereignty"

Public international law defines sovereignty as a state's exclusive competence over its territory, including land, corresponding subsoil, territorial sea (defined in nautical miles from the shore) and airspace (delimited by vertical extension of land and sea borders).[11] Sovereignty thus rests on a spatial legal regime where location is legally determinative. However, in the virtual world of information and communications technology (ICT) and artificial intelligence, delineating sovereignty becomes difficult. Physical digital infrastructure (servers, wireless networks, databases) may be located in one state's territory, but data processing activities may occur in, or relate to individuals in another state's territory. Cyberspace has no definite borders. When multiple states have concurrent sovereignty claims over ICT, conflict of laws rules come into play to define the scope of each state's jurisdiction.

Relevant to data sovereignty, public international law imposes a duty on states to protect their citizens' human rights.[12] The GDPR provisions governing transfers of personal data outside the European Union, designed "to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined,"[13] align with this fundamental principle of international law.

2. Rules of conflict of laws governing the scope of jurisdiction

a. Context

While state sovereignty protects a state's exclusive decision-making powers over its territory, jurisdiction refers to the specific rights, liberties and powers inherent to sovereignty.[14] Some states, such as the UK, US and Australia, apply a presumption against extraterritoriality, meaning that a statute is presumed not to apply extraterritorially unless it explicitly says so or does so by necessary implication. Other states, such as Canada and EU member states, rely on the territorial nexus doctrine, meaning any substantial connection with a state's territory may bring a matter under that state's jurisdiction. In the data context, one recurring common factor is whether an entity subject to the forum's jurisdiction has possession, custody, or control of the data. The doctrines can diverge, however, when data is held in another state.

11. Ian Brownlie Principles of Public International Law at page 109.
12. *See, e.g., Guiding Principles on Business and Human Rights*, U.N. HUM. RTS. OFF. OF THE COMM'R (2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
13. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation, art. 44, 2016bO.J. (L 119) 33 [hereinafter GDPR].
14. *Id.*, at page 110.

b. The evolution of jurisdiction over data

Data sovereignty claims in the borderless realm of cyberspace inevitably raise concerns about extraterritorial jurisdictional reach. The first major tension arose with the adoption of the *General Data Protection Regulation* (GDPR) in 2016, which applies the territorial nexus doctrine. The GDPR asserts jurisdiction over organizations not established in the EU where the processing activities relate to offering goods or services to data subjects in the EU or monitoring their behaviour in the EU.[15]

The debate intensified in 2018 when the US adopted the *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, which amended the *Stored Communications Act* (SCA) to require covered providers of electronic communication service or remote computing service to preserve, back up or disclose data within their possession, custody or control in response to valid US legal process, regardless of whether the data is located inside or outside the US.[16]

The latest development raising concern is the September 19, 2025, decision of the Ontario Court of Justice in *The King v. OVH*,[17] which confirmed the application of a production order issued under Canadian law over data held in France. The decision is currently under appeal, but given the urgency surrounding digital and AI sovereignty, the trial court's reasoning remains highly relevant.

c. The Ontario Court of Justice decision in *The King v. OVH*

Under Canadian law, jurisdiction extends to any matter with a "meaningful connection" to Canada-including a virtual connection, or in other words, a "real and substantial link." In *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*[18], the Supreme Court of Canada established that a "real and substantial link" does not require a foreign organization to have a physical presence in Canada "because telecommunications occur 'both here and there'."[19] The Court identified the key connecting factors of jurisdiction as "the location of the content provider, the end user and the intermediaries, in particular the host server," noting that "[t]he location of the end user is a particularly important factor."[20] Jurisdiction over internet activities therefore extends beyond territorial borders, with rules on conflict of laws governing its scope.

In *The King v. OVH*, the Court asserted Canadian jurisdiction over a Criminal Code production order (issued under s. 487.014) requiring subscriber and account data linked to four IP addresses associated with OVH Groupe SA (OVH Parent) and Hébergement OVH Inc. (OVH Canada). The data was held on OVH servers in France, the United Kingdom and Australia. OVH Parent, headquartered in France, has subsidiaries in France, the UK and Australia. The production order was issued in the context of a national security investigation.

OVH Parent operates data centres in Québec and Ontario through OVH Canada, and OVH Canada has technological access to data held by OVH Parent. The validity of the production order turned on three issues: (i) does OVH Canada have "possession or control" over the requested data?; (ii) does the Canadian court have jurisdiction over OVH Parent?; and (iii) do any limitations apply to the extraterritorial application of Canadian law?

15. GDPR, Article 3(2).
16. 18 U.S.C. § 2713.
17. COURT FILE No: 24-000659
18. *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45 (CanLII), [2004] 2 SCR 427
19. *Id.*, at para. 59
20. *Id.*, at para. 37

The Court found that OVH Canada has possession or control of the requested data because, as part of a single corporate group with global offices, it has access to data held in France. The Court also found it had jurisdiction over OVH Parent because its Canadian operations constitute a "meaningful connection" to Canada.[21]

OVH Parent invoked two limitations to counter the extraterritorial application of the Canadian production order. First, it argued that compliance would violate the French Blocking Law (Law No. 68-678 of July 26, 1968), which restricts the communication of economic, commercial, industrial, financial or technical information to foreign persons or entities.[22] The Court dismissed this argument, finding that the French Blocking Law did not create a real risk of prosecution given its scope (protecting data critical to French state interests, not privacy) and its lack of enforcement. Second, OVH Parent argued that an alternative process existed in the Mutual Legal Assistance Treaty (MLAT). The Court dismissed this argument as well, finding the MLAT process too "slow and uncertain" to be effective "in an era when information moves instantaneously and may be stored only for a short time."[23] The court relegated the MLAT process to a time when evidence was physically confined to a territory, requiring mediation of the state authorities of that territory to access it.

Looking to the future, the Court opened the door further to extraterritoriality. Adopting the view in *Attorney General v. Brecknell*,[24] it stated: "I do not think that a principled effective system of legitimate investigation based on international norms should be contingent on business decisions taken by service providers in their own private interest."[25] Yet, as discussed below in the section on legal measures to assert digital and AI sovereignty, the protection of digital and AI sovereignty rests precisely on corporate decisions regarding data governance.

d. Comparing the OVH decision with the *CLOUD Act*

The OVH decision invites comparison with Microsoft litigation. In that case, the Second Circuit held that a warrant under the SCA did not compel Microsoft to produce email content stored in Ireland.[26] Before the Supreme Court could reach the merits of the government's appeal, Congress enacted the *CLOUD Act* (March 2018); the Supreme Court then vacated the Second Circuit's judgment and remanded with instructions to dismiss as moot (per curiam, April 17, 2018). The Second Circuit's reasoning nevertheless illustrates the US presumption against extraterritoriality as it applied to the pre-*CLOUD Act* SCA. The key distinction from the Canadian decision is that Canada does not apply a presumption against extraterritoriality. Instead, it applies the territorial nexus doctrine, grounding jurisdiction in a real and substantial link to Canada, regardless of where the data is stored.

The Microsoft litigation helped precipitate Congress's adoption of the *CLOUD Act* in March 2018, which added 18 U.S.C. § 2713 to the SCA, removing it from the presumption against extraterritoriality, and bringing it into line with the territorial nexus doctrine: any business link with the US may extend US authorities' jurisdiction to data held outside the United States. The legislative change triggered global anxiety that has often obscured the *CLOUD Act's* actual scope and impact. In "The *CLOUD Act*: What It Is – And What It Isn't,"[27] Microsoft provides clarification:

- The *CLOUD Act* serves two purposes: (i) clarifying the legal authority of US government entities to seek cross-border data, and (ii) authorizing the US Government to conclude bilateral agreements allowing reciprocal direct access to locally held data. To date, only the United Kingdom (signed 2019; entered into

21. *The King v. OVH*, Court File No. 24-000659, at para. 13.
22. *Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, at* https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326
23. *The King v. OVH*, Court File No. 24-000659,
24. 2018 BCCA 5.
25. *Attorney General v. Brecknell*, 2018 BCCA 5, at para. 102
26. *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), *vacated as moot, United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018)) (*per curiam*).
27. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/CLOUD-Act-What-it-is-and-is-not.pdf.

force October 3, 2022) [28] and Australia (signed December 15, 2021; entered into force January 31, 2024) [29] have concluded such agreements with the US. Formal negotiations with Canada (commenced 2022) and the European Union (resumed 2023) are ongoing.

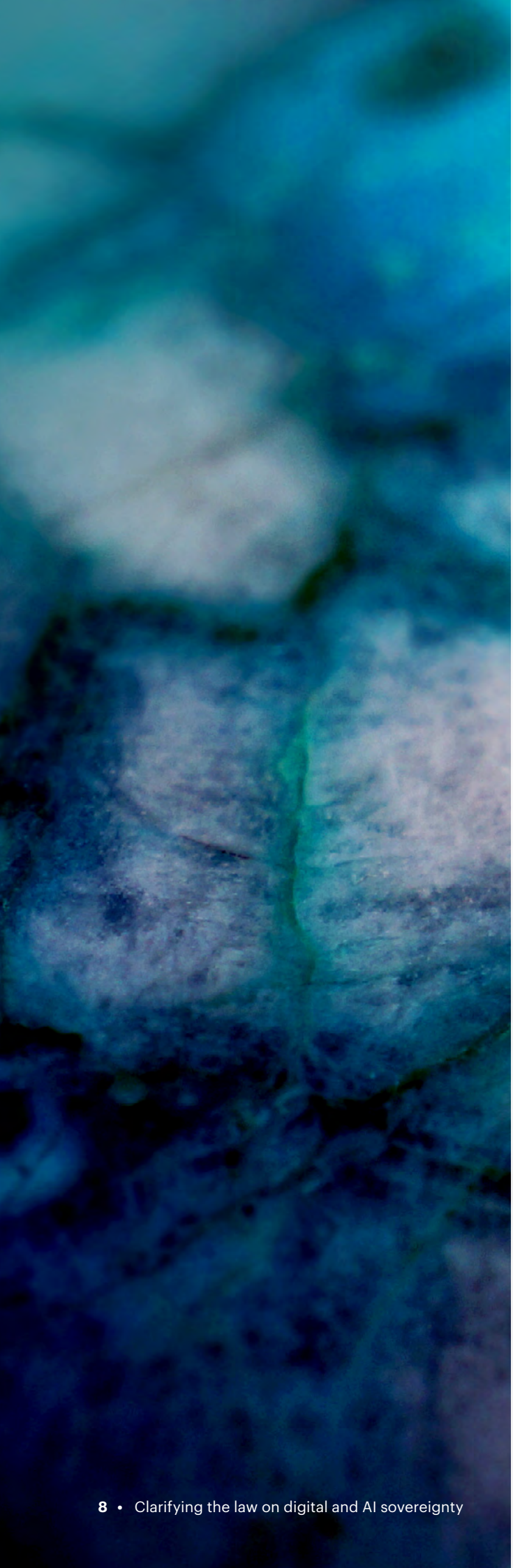
- The *CLOUD Act* does not eliminate existing legal requirements for data access. The government must still obtain a warrant or court order subject to judicial approval, demonstrating to the court that there is reason to believe evidence of crimes will be found in the specified account data.
- The *CLOUD Act* recognizes a limited statutory mechanism for a covered provider to move to quash or modify process seeking content where, among other requirements, the subscriber or customer is not a US person and does not reside in the United States, and compliance would create a material risk of violating the laws of a qualifying foreign government; the court then applies specified comity factors.
- Extraterritorial law enforcement access to data is not unique to the CLOUD Act. National laws, and international conventions, recognize the authority of a state to access data held abroad in certain circumstances and under strict legal requirements.
- Perhaps most importantly, the CLOUD Act's scope is not limited to US companies, but it does not reach a provider with no jurisdictional connection to the US. The statute applies to covered providers of electronic communication service or remote computing service that are subject to US legal process and have possession, custody or control of the requested data.

Canadian law and the *CLOUD Act* can create comparable practical conditions for extraterritorial application of domestic law:

- An organization that has activities in the country issuing a data production order, such as offering services, may come under the jurisdiction of the issuing country.
- If the organization has a local presence, such as an affiliate, in the country issuing the order and the local affiliate has control or access to the foreign held data, it may be compelled to produce that data.
- If the organization has no local affiliate in the issuing country, law enforcement authorities must proceed through international cooperation to serve an order to produce foreign held data.

On June 10, 2025, during an appearance before the French Senate,[30] Microsoft France's Director of Public and Legal Affairs, Anton Carniaux, stated that Microsoft would comply with a lawful production order, including from the US. He was accurately stating the law. The storm his remarks created reveals the misconceptions about foreign lawful access: it is not off-limits but rather subject to privacy laws governing state access to personal data across borders.

28. Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, signed October 3, 2019, https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern.
29. Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, U.S-U.K-N. Ir., Oct. 3, 2019, available at https://www.justice.gov/criminal/media/1076581/dl?inline#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes.
30. https://www.senat.fr/actualite/commande-publique-audition-de-microsoft-5344.html.



3. Data sovereignty through privacy law on cross-border data flows

Data may be subject to the laws of more than one state, depending on the applicable connecting factors, including where it is stored or processed, where the relevant individuals or activities are located, and which entity has possession, custody or control of the data. States prohibit, restrict or impose varying conditions on cross-border data flows to protect data sovereignty.

The GDPR is the reference point for legal regimes on cross-border data flows. Chapter 5 subjects personal data transfers outside the EU to specific conditions:[31] Article 45 allows transfers to countries with "an adequate level of protection" (equivalent to that provided in the EU), while Article 46 subjects other transfers to "appropriate safeguards" – most commonly, the standard contractual clauses (SCCs) adopted by the European Commission. The GDPR itself, in Recital 109, recognizes that "controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses,"[32] reflecting the concern, expressed in Recital 116, that "[w]hen personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders."[33] In *Schrems II* (Case C-311/18, CJEU, 16 July 2020), the Court of Justice of the European Union gave these concerns operative effect, invalidating the EU-US Privacy Shield and holding that exporters relying on SCCs must assess, on a case-by-case basis, whether the law and practice of the importing country afford essentially equivalent protection and, if not, adopt supplementary measures. Since then, the European Commission has adopted a successor adequacy decision — the EU-US Data Privacy Framework (Commission Implementing Decision of 10 July 2023) — which permits transfers to certified US organizations subject to the Framework's commitments on limitations on US intelligence

31. GDPR, Article 44.
32. GDPR Recital 109, Regulation (EU) 2016/679; Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, judgment of July 16, 2020.
33. GDPR Recital 116, Regulation (EU) 2016/679; Schrems II, Case C-311/18.

access and redress mechanisms. Articles 46(2)(b) and 47 of the GDPR also permit transfers on the basis of binding corporate rules ("BCRs") approved by the competent EU supervisory authority. While the GDPR does not legally extend EU jurisdiction to third countries, it asserts data sovereignty by requiring an EU-equivalent legal regime, statutory or contractual through the SCCs or the BCRs, before a third country may receive EU personal data.

Modeled on the GDPR, but accounting for the need for free circulation of personal data in the integrated North American economy, Québec's *Act respecting the protection of personal information in the private sector* was modernized in 2021 to strengthen conditions on cross-border data flows. Before communicating personal information outside Québec, a person carrying on an enterprise must conduct a privacy impact assessment that takes into account the sensitivity of the information, the purposes for which it is to be used, the protection measures that would apply, including contractual measures, and the legal framework applicable in the receiving jurisdiction. The communication may proceed only if the assessment establishes that the information would receive adequate protection, and the communication must be subject to a written agreement reflecting the assessment and any risk-mitigation terms.[34] Like the GDPR, this provision does not legally extend Québec's jurisdiction but asserts data sovereignty by requiring that transferred personal data remain subject to an equivalent legal regime.

The US, while generally committed to free cross-border data flows, issued Executive Order 14117 in 2024. The DOJ implementing rule prohibits or restricts specified covered data transactions that would give countries of concern or covered persons access to US government-related data or bulk US sensitive personal data, subject to thresholds, exemptions, licensing, and compliance requirements.[35] The policy behind the Executive Order is an exercise of US data sovereignty.

The French Blocking Law, invoked in *The King v. OVH*, is another example of legislation asserting data sovereignty. Adopted in 1968, it prohibits any person or entity under French jurisdiction from communicating economic, commercial, industrial, financial or technical information to foreign state authorities if such communication could harm French sovereignty or interests, except as allowed by international treaties. Violations are punishable by imprisonment and fines.

International trade agreements also protect data sovereignty while facilitating cross-border personal information flows. Chapter 19 of the Canada-United States-Mexico Agreement (CUSMA) binds the parties not to restrict or prohibit cross-border electronic transfer of information, including personal information, in the conduct of business. However, parties may adopt measures inconsistent with that rule if necessary to achieve a legitimate public policy objective, provided the measure is not applied as arbitrary or unjustifiable discrimination or a disguised restriction on trade and does not impose restrictions on transfers greater than necessary to achieve the objective.[36] Similarly, the Comprehensive Economic and Trade Agreement (CETA) between Canada and the EU creates exceptions to its trade-facilitating provisions for the protection of individual privacy in relation to the processing and dissemination of personal data.

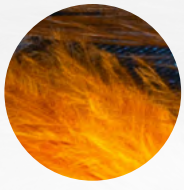
With the global expansion of ICT use, restrictions on cross-border data flows have increased principally due to personal data protection concerns. These restrictions range from legal regimes governing cross-border data flows, to government procurement policies requiring local data centres, private sector contractual clauses mandating local storage and to outright bans on communicating data abroad. The trend continues, with more states implementing restrictions. The OECD confirms that data localisation requirements are growing and becoming increasingly restrictive, with close to a hundred data localisation measures across 40 countries in place by early 2023 and more than half of those measures emerging since 2015.[37]

34. Québec *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, s. 17 (Can.).
35. US Department of Justice, National Security Division, Final Rule, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 90 Fed. Reg. 1636 (January 8, 2025), https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.
36. Canada-United States-Mexico Agreement, Can.-U.S.-Mex., Nov. 30, 2018, at Article 19.11 [hereinafter CUSMA].
37. Chiara Del Giovane, Janos Ferencz, and Javier Lopez-Gonzalez, *The Nature, Evolution and Potential Implications of Data Localisation Measures*, OECD (2023), https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf.

4. The legal measures to assert digital and AI sovereignty

As noted at the outset, digital and AI sovereignty is not merely a matter of government investments or policy direction; it is a matter of public international law and conflict of laws rules and it may not be achievable. The convergence of legal rules and the centralization of digital and AI technological infrastructure in a few states make asserting digital and AI sovereignty challenging. For businesses, it requires a technological and corporate structure that precludes international access, which may or may not be feasible depending on the business model. We address this issue and identify the legal conditions for digital sovereignty in our article "The privacy advantage of Canadian data centres." The decision in *The King v. OVH* confirms our description of the corporate structure needed to achieve data sovereignty and illustrates its elusiveness:

- **Local technological infrastructure to support local operations:** In the increasingly rare case where an organization's market is entirely within one state, it could escape extraterritorial reach by relying on technological support with no ties to any foreign company. Few business models fit this operational reality.
- **Operational segregation:** Most organizations operate in more than one state, directly or through affiliates. Affiliates fall under the jurisdiction of the state where they operate. Data can be shielded from direct foreign access and require international cooperation through an MLAT only if the affiliate has no technological access to the requested data. This requires internal segregation: administration, identity management and encryption key management must reside entirely in the parent company's state, with technical and organizational measures preventing affiliates from accessing the parent's data. The administrative challenges are obvious.
- **Independent corporate or contractual control:** Even without affiliates or operations in foreign countries, organizations may be controlled by foreign entities holding equity in the company. These entities fall under the jurisdiction of their state of incorporation. Through their decision-making powers, they have control over data held by the company (even data in another country) and may be compelled to produce it. Corporate governance can address this risk by excluding foreign entities from corporate or contractual control. "Control" includes the right to access or direct production of corporate data, whether through board-level policies, unilateral directives, shared credentials or "books and records" clauses extending to tenant data. Protective governance structures would exclude foreign entities from any direct or indirect access, custody or decision-making power over the organization's data.
- **Limiting US contacts under the *CLOUD Act*:** To reduce CLOUD Act exposure, an organization should assess whether it is a covered provider subject to US legal process and whether requested data would be within its possession, custody or control. The absence of US offices, agents for service, targeted US marketing, US affiliates or US ownership may reduce the jurisdictional hook, but US authorities could still obtain access to data through a US-based provider with custody or control or through international cooperation mechanisms such as a Mutual Legal Assistance Treaty.



5. Managing compliance with extraterritorial access requests

Truly "sovereign" databases will be rare: an affiliate, service provider or service offering in another country could all provide grounds for foreign jurisdiction. Organizations must therefore be prepared for due diligence in managing extraterritorial access requests. Key measures include:

- Transfer impact assessments: As identified in Schrems II and required under Québec's Act respecting the protection of personal information in the private sector (discussed above in the section on privacy law and cross-border data flows), transfer impact assessments should precede any cross-border data transfer to a country with broad state access rights to personal data.
- Cross-border data transfer mitigating measures: Data protection clauses in service agreements or intra-group agreements may mitigate the impact of foreign access requests:
    - Transfer may be limited to access, no storage, with restricted privileges and audit trails.
    - Technological safeguards may be required to guard against direct state access.
    - Service providers or affiliates should be required to submit to the customer or parent organization any state access request to assess its lawfulness and either approve compliance or challenge it.
    - If operationally possible, transfers could be limited to de-identified or anonymized information meaning that the information transferred is severed from identifiers maintained locally (de-identified), or that the identifiers are destroyed in a manner that makes the information no longer traceable to an individual in an irreversible manner (anonymized).
- Understanding rights and obligations regarding lawful access: Whether through in-house counsel or external advisors, organizations should have resources to guide them in assessing the lawful authority of a government institution to demand access to personal data:
    - Does the foreign country institution have jurisdiction?
    - If so, is the demand lawful under the laws of that country?
    - Do any local blocking laws impede providing access as demanded?

The upshot

The Canadian decision in *The King v. OVH* brought to light the principles of public international law that determine the scope of digital and AI sovereignty, revealing its limits. To protect their data holdings from extraterritorial access and make valid commitments to data subjects, organizations must understand the limits of their control over foreign lawful access and the legal and operational strategies that can maximize it.

For more information, please contact the authors, listed below.

*From Dentons Canada, **Chantal Bernier**, Co-chair of the Global Privacy and Cybersecurity group*

*From Dentons US, **Todd Daubert**, Chair of the Communications and Technology, Lead of the US Privacy and Cybersecurity group, and Leader of the Global Technology, Media and Technology Sector*

Key contacts

Chantal Bernier
Of Counsel
Ottawa
D+1 613 783 9684
chantal.bernier@dentons.com

Todd Daubert
Partner
Washington, DC
D+1 202 408 6458
todd.daubert@dentons.com

ABOUT DENTONS

Redefining possibilities. *Together, everywhere.* For more information visit **dentons.com**

CSBrand-195799-Clarifying the law on digital and AI sovereignty Brochure-02 — 07/05/2026