HUMAN TECHNOLOGY FOUNDATION

ITECHLAW®
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

TECHNOLOGY SOVEREIGNTY REPORT

A survey of middle powers' converging drivers and mitigation strategies to adress technological sovereignty vulnerabilities

Led by **CHARLES MORGAN**
ITECHLAW

& **ERIC SALOBIR**
Human Technology Foundation

June 2026

Table of Contents

Human Technology Foundation: Since 2012, the Human Technology Foundation has worked as an independent think and do tank focused on keeping humanity at the center of technological progress and its responsible oversight. We believe technology should be part of the broader social conversation, not separate from it.

ITechLaw: ITechLaw has been serving the technology law community worldwide since 1971. It has a global membership base representing six continents and spanning more than 70 countries. Its members and officials reflect a broad spectrum of expertise in the technology law field. Its mission is to create unparalleled opportunities for international networking and exchanging knowledge and experience with experts and colleagues around the world.

This report does not provide legal advice. It is provided for informational purposes only.

Each of the contributors to this report has participated in its drafting on a personal basis. Accordingly the views expressed do not reflect the views of any of the companies, law firms or other entities with which they may be affiliated.

Firm names and logos, while used with permission, do not necessarily imply endorsement of any of the specific views and opinions set out herein.

The contributors have worked diligently to ensure that all information in this report is accurate as of the time of publication. The Human Technology Foundation will gladly receive information that will help, in subsequent editions, to rectify any inadvertent errors or omissions.

Preface

One year after the publication of the Draghi Report, the European Union and other middle powers remain exposed to significant technological vulnerabilities and critical dependencies. Seeking to position themselves as strategic powers and genuine business partners rather than mere markets for global competitors, middle powers have come to understand that full technological sovereignty (understood as complete economic and military independence) is neither realistic nor achievable in the short to medium term. Moreover, they understand that such an outcome is ultimately undesirable, since a "go it alone" approach would make suboptimal use of global resources.

Across a number of foundational domains such as artificial intelligence, data, cloud computing, digital infrastructures, networks, and access to space, fully sovereign alternatives either do not yet exist or cannot be deployed without prohibitive costs or substantial losses in performance. This reality calls for a shift in perspective. The challenge is no longer only to close industrial gaps, but to safely manage structural and enduring technological interdependencies.

Thus, States and large corporations have little choice but to anticipate worst-case scenarios and to systematically assess their technological vulnerabilities that could be subject to "weaponization." Whether through the risk of embargoes, excessive reliance on suppliers able to exploit dominant positions, or large-scale data loss, exposure, or seizure, these vulnerabilities now constitute significant risks in their own right.

As a result, the core issue is no longer limited to the question of what should be produced domestically or within middle powers, but increasingly concerns how to continue using state-of-the-art technologies—including foreign solutions—without exposing middle powers to systemic risks.

It is from this observation that the present document emerges. We have undertaken this work within the framework of an initiative led by the Human Technology Foundation, with the collaboration of members of ITechLaw. This document has been developed with the active contribution of lawyers from across the ITechLaw network, whose expertise has informed both the legal analysis and the identification of concrete vulnerabilities. Together, we bring perspectives from multiple jurisdictions, with a deliberately pragmatic objective: to identify, assess, and prioritize technological vulnerabilities in order to explore concrete and actionable means of mitigating them.

This document goes beyond a simple inventory of threats. It proposes a structured approach starting from legal vulnerabilities that may affect data protection, control over critical infrastructures, or even freedom of action. Based on this mapping, it aims to facilitate the identification of available mitigation levers such as technical architectures and mechanisms or operational organizations capable of reducing exposure to risk without sacrificing performance or innovation.

This work is primarily intended for public decision-makers, C-suite of large international companies, legal departments, IT and cybersecurity leaders facing these complex trade-offs. It does not seek to prescribe a single path or to frame sovereignty and performance as opposing objectives, but rather to provide analytical and practical tools to support informed decision-making. In this sense, the document is designed as a decision-support instrument for economic actors operating in an environment where technological interdependence is unavoidable, but must be carefully managed.

The following pages present the methodology adopted and the initial results derived from eight country reports (set out in the annex to this report) assessing technological sovereignty through the lens of applicable legal and policy frameworks. This report represents a first step of a two part process, which will be further refined, expanded, and challenged, notably through a forthcoming technical/operational report on mitigation strategies designed to help decision-makers to better understand their technological dependencies, prioritize them, and determine which must be redressed, mitigated, or accepted.

Eric Salobir
Human Technology Foundation

Charles Morgan
ITechLaw

Technological Sovereignty Report:

A Survey of middle powers' converging drivers and mitigation strategies to address technological sovereignty vulnerabilities

Introduction

Across a range of "middle power" countries, three distinct factors are converging to elevate technological sovereignty from an abstract aspiration to a practical policy agenda:

- National security imperatives
- Economic security concerns
- The desire to protect fundamental democratic values.

A broad range of recent geopolitical shifts have transformed technological dependencies on foreign technology stacks into full-fledged national security risks for middle powers. The battle over global dominance in frontier artificial intelligence (AI) has essentially become an "arms race" between the United States and China, with Europe and other middle power jurisdictions largely relegated to the sidelines, increasing reliant on foreign actors. The Trump administration has signaled a dramatic shift in the US national security posture and has asserted territorial ambitions that would have been, until recently, almost unthinkable[1][2]. In this context, the war in Ukraine has exposed how critical digital infrastructure can be subject to private control and geopolitical leverage (e.g., the highprofile limitation of satellite connectivity), while allied procurement dependencies have underscored how foreign export controls can constrain sovereign defense choices even when alternatives exist.

In parallel, shifting trade dynamics, sanctions, and an increasingly transactional global order are pushing governments to seek resilient access to core technologies and to diversify away from single points of failure. Many middle powers have come to realize that their reliance on the technology stack of foreign powers means that they have been essentially left on the sidelines of value creation, productivity improvements and explosive economic growth as artificial intelligence and other disruptive technologies continue to transform the global economy.

Finally, a deep-seated desire to protect fundamental values such as privacy, due process and pluralism has been reignited by a long series of surveillance scandals (e.g the Snowden disclosures on PRISM[3]), data misuse episodes (e.g. Cambridge Analytica[4]), and the stepchange impact of generative AI since late 2022, all of which focus attention on who controls data, computing capacity, and platform rules.

In this context, middle powers are converging on a working definition of technological sovereignty as strategic autonomy in decisionmaking and sufficient control over key technological infrastructure to maintain the ability to act autonomously, especially in times of crisis, while remaining open, interoperable, and competitive.

1 The White House, *National Security Strategy of the United States of America*, The White House, November 2025, available online: 2025-National-Security-Strategy.pdf
2 Chris Cameron, "Trump Threatens to Take Greenland 'the Hard Way'", *The New York Times*, January 2026, available online: Trump Threatens to Take Greenland 'the Hard Way' - The New York Times
3 Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 7 June 2013, available online: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
4 Federal Trade Commission, *In the Matter of Cambridge Analytica, LLC, Docket No. 9383: Opinion of the Commission*, Federal Trade Commission, 25 November 2019, available online: https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf

In practice, this translates into initiatives to invest in domestic high performance compute capacity and reduce exposure to foreign data disclosure legal regimes, overreliance on dominant platforms and supplychain chokepoints, without retreating into isolationism. It also reflects a sectoral prioritization logic: sovereignty levers are applied most strongly to sensitive publicsector data, securityrelevant infrastructure, health data, and highimpact AI systems, while general commercial activity remains globally integrated.

The threats animating this agenda typically fall into four buckets.

- **First,** unchecked, concentrated market dominance by a handful of foreign actors can entrench dependency and limit the ability of a country's domestic firms to scale, impeding competitiveness.
- **Second,** coercive trade or sanctions pressure can accentuate economic vulnerabilities and constrain domestic policy choices.
- **Third,** legal uncertainty as regards the rights of creators in content that is used, massively, to train AI models, has resulted in a massive concentration of economic value in the hands of a relatively limited number of market players.
- **Fourth,** extraterritorial data access regimes (e.g., US CLOUD Act; intelligence collection frameworks) threaten to bypass local due process and undermine public trust.

In response, surveyed countries rely on a toolbox of legislative measures and policy initiatives.

To counter dominance and reduce lockin, competition laws and platform rules are central. The EU's Digital Markets Act[5] imposes interoperability, data access/portability, and antiselfpreferencing obligations on gatekeepers, a stance echoed by active national enforcement that pushes for fair consent design and clearer datause choices. In parallel, publicsector cloud strategies emphasize hybrid/multicloud architectures and supplier diversification to prevent singlevendor dependence. Switzerland's federal multicloud model exemplifies this approach.

Trade and procurement levers complement these measures: while formal "buy local" mandates are often constrained by trade commitments, national security carveouts, investment screening (e.g., Italy's Golden Power), and project level conditions allow states to block sensitive acquisitions, favour "trusted" infrastructure, and anchor strategic capabilities at home. In addition, industrial policy and tax incentives support endogenous capacity building: France 2030[6] and High Performance Computing (HPC)/AI programs, Italy's R&D credits, Argentine Knowledge-Economy Promotional tax Regime[7] and Promotion and Development of Technological Innovation Law[8] (focused on R&D and human capital rather than compute infrastructure), Switzerland's R&D superdeduction, and Canada's SR&ED all tie fiscal support to domestic R&D and infrastructure, while targeted AI/quantum/HPC investments expand compute and research ecosystems.

As regards the issue of rights in the content used as training data for large language models and in the content that is produced as outputs of such models, both courts and legislators continue to struggle to find the right balance between protecting rights-holders in relation to the training data used to train large language models and promoting innovation and the societal benefit that such LLMs are unleashing. As cases move through the courts, legislators across middle power countries are considering right-sized law reform, especially in relation to copyright under "fair use" and "fair dealing" principles, as well as text and data mining (TDM) exceptions.

On data protection and lawful access, the throughline is judicial oversight and a rejection of bulk or indiscriminate collection for ordinary access regimes, with any exceptional intelligence collection placed in a special, controlled framework. Crossborder transfers are conditioned on adequacy or safeguards, with additional blocking statute style constraints channeling foreign requests through MLATs or eevidence instruments. Governments classify and segment data (e.g., Canada's Protected vs. Classified levels and similar publicsector stratifications in European Union member states), tie sensitive workloads to "trusted/sovereign" clouds, and use public sector procurement to steer toward providers meeting security certifications (e.g., France's SecNumCloud) or national/EU hosting commitments (e.g., Italy's Polo Strategico Nazionale for public administrations). Enforcement actions, including against unlawful analytics transfers, signal that sovereignty risks are not theoretical but carry compliance consequences.

Taken together, these measures show that countries implementing technological sovereignty do not seek autarky. Rather, they aim to ensure that, when push comes to shove, when faced with military threats, economic coercion, or foreign laws affecting the fundamental rights of their citizens, they retain lawful, practical, and credible freedom of action. The post Ukraine war security landscape, the end of globalization drift, the privacy shocks of the last decade, and the generative AI inflection point have all accelerated this shift.

5 European Commission, "About the Digital Markets Act", *Digital Markets Act (DMA)*, European Commission, available online: https://digital-markets-act.ec.europa.eu/about-dma_en

6 French Government, "Understanding France 2030", *France 2030*, info.gouv.fr, 7 May 2024, available online: https://www.info.gouv.fr/grand-dossier/france-2030-en/understanding-france-2030

7 Argentine Law 27.570, in force until 2029, is a tax incentive program that aims to promote new technologies, facilitate the developments of Micro, Small and Medium-sized Enterprises and increase exports of companies engaged in knowledge-based services

8 Argentine Law No. 23,877, provides, among other benefits, Argentine companies investing in R&D and technological innovation may be eligible for a tax credit bond equivalent to a percentage of the expenses incurred in this field

9 MB Group Switzerland AG, "The Swiss Patent Box", *Company Swiss*, available online: Switzerland's patent box – Company Swiss

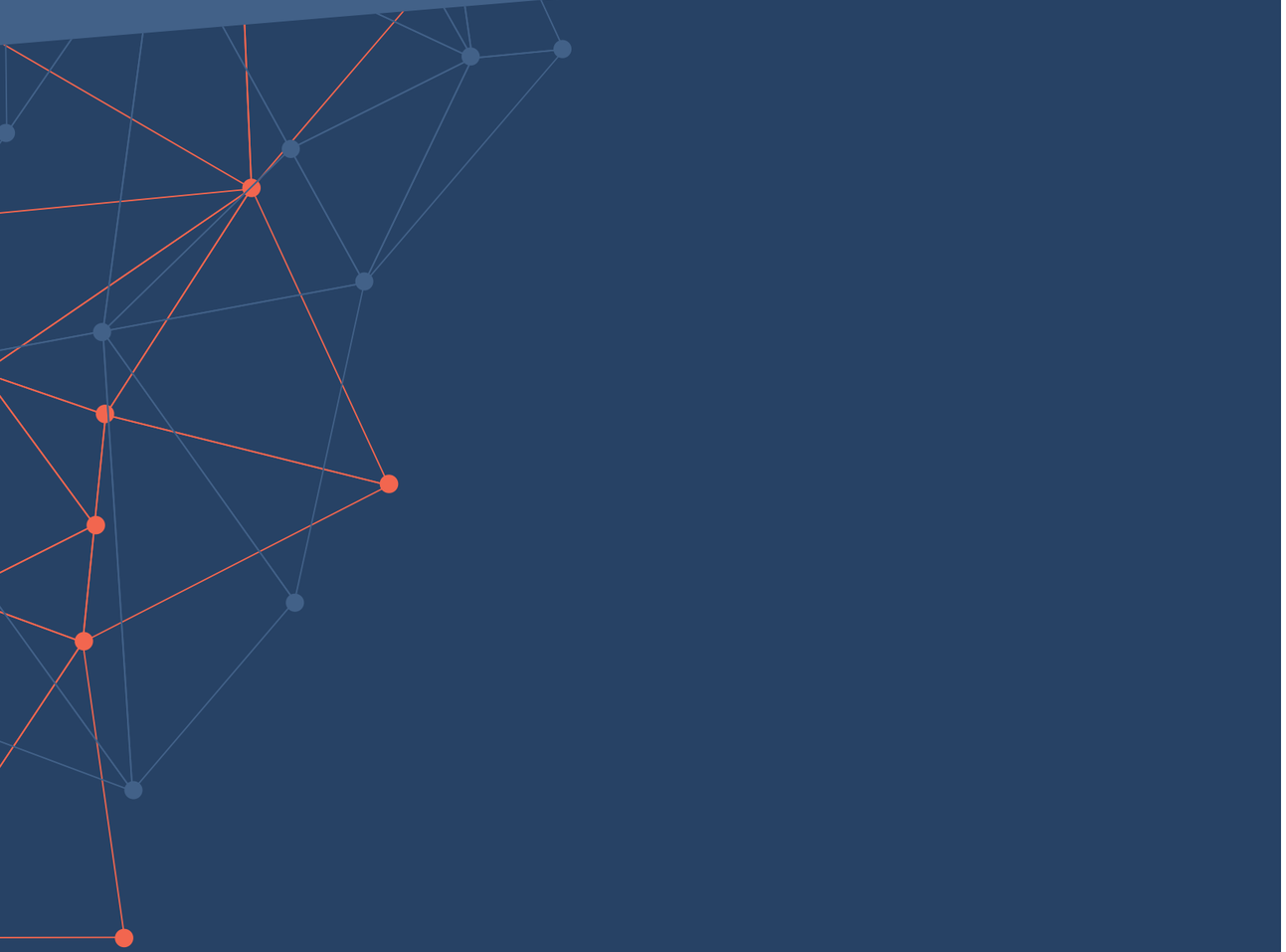
10 Canada Revenue Agency, "Scientific Research and Experimental Development (SR&ED) tax incentives", *Canada.ca*, Government of Canada, available online: https://www.canada.ca/en/revenue-agency/services/scientific-research-experimental-development-tax-incentive-program.html

11 Agence nationale de la sécurité des systèmes d'information (ANSSI), "Cloud", *ANSSI*, French Government, available online: https://cyber.gouv.fr/enjeux-technologiques/cloud/

12 Department for Digital Transformation and National Cybersecurity Agency, "Polo Strategico Nazionale", *Cloud Italia*, Italian Government, available online: https://cloud.italia.it/strategia-cloud-pa/polo-strategico-nazionale comm_final_opinionpublic.pdf

Part 1

Converging Policy Drivers for Technological Sovereignty



1 - National Security

The national security dimension of technological sovereignty has increased in importance not only because of dramatic changes in US foreign policy calling for its NATO partners to assume primary responsibility for their regions' defence[13], but also because recent crises have made visible, often in operationally consequential ways, that critical digital infrastructure can be selectively withheld, constrained, or reconfigured by private actors or foreign states at decisive moments. In Ukraine, battlefield connectivity became dependent on a privately operated satellite network and media reported an episode in late September 2022 where coverage was shut off in key frontline areas during a Ukrainian counteroffensive, producing a communications blackout that reportedly affected drone operations, artillery targeting, and frontline[14] coordination. This scenario collapses the traditional distinction between "civilian" infrastructure and "defence" infrastructure: the same cloud tenancy, satellite constellation, identity provider, or update channel may be simultaneously a commercial product and a key component of systems used in national security operations.

A parallel vulnerability arises from the sanctions and export-control environment, where digital service access can become an instrument of foreign policy. In a widely noted example, the International Criminal Court's chief prosecutor and staff reportedly had their access to Microsoft email and services suspended following the application of U.S. sanctions, illustrating that a major provider can disrupt services "in direct response to US government sanctions."[15] Although Microsoft has denied that it was involved in the suspension of service to ICC officials[16], this episode demonstrates the risk that foreign technology providers may be required to comply with directives from their jurisdiction or origin. For middle powers, the risk is amplified by the fact that many lack homegrown technology providers, including national hyperscale cloud platforms and satellite communications champions.

Defence procurement dependencies are a particularly stark subset of this broader pattern. Where advanced weapons platforms are software-defined and sustainment-intensive, "autonomy" is less about the physical hardware than the ongoing ability to patch, upgrade, certify, and maintain mission capability. In the Canadian, German and Norwegian debates around next-generation fighter jets, for example, concerns were raised that the United States "controls all software upgrades" for the F-35

13 The White House, *National Security Strategy of the United States of America*, The White House, November 2025, available online: 2025-National-Security-Strategy.pdf

14 *News18*, "Elon Musk Ordered Starlink Shutoff During Ukraine Offensive, Disrupting Frontline Ops: Report", *News18*, available online: https://www.news18.com/world/elon-musk-ordered-starlink-shutoff-during-ukraine-offensive-disrupting-frontline-ops-report-ws-l-9463885.html

15 Owen Sayers, "Microsoft's ICC email block reignites European data sovereignty concerns", *Computer Weekly*, 23 May 2025, available online: https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns

16 Sam Clark, "Microsoft didn't cut services to International Criminal Court, its president says", POLITICO, 4 June 2025, available online: https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/

and that "without those upgrades, no country can hope[17] [18] to operate the [aircraft] for long." Even where the existence of a literal "kill switch" is denied, the practical leverage of the dominant technology provider is structural: dependence on a controlled logistics network, proprietary parts, and software support can create a scenario where capability is gradually degraded if political relations sour[19]. In other words, procurement choices can embed foreign-policy contingency into the operational lifecycle of core national defence capabilities. The sovereignty question therefore extends beyond "who supplies" to "who can keep it running," "who can audit or certify it," and "who can change it" under conditions of diplomatic friction[20].

Taken together, these dynamics explain why "national security" threats in technological sovereignty debates are no longer limited to espionage and sabotage. They include service continuity risk (denial or degradation of essential digital services), coercive sanctions and export controls, and lifecycle dependencies embedded in software that affect public procurement options. The policy response emerging across middle powers is correspondingly pragmatic: reduce single points of failure, impose national security certification and jurisdictional control requirements for sensitive workloads and data, harden contractual protections around continuity and access, and invest in domestic or allied capacity in the layers (cloud, compute, security operations, and maintenance ecosystems) that determine whether sovereignty is actionable when tested.

2 - Economic Security

As noted by Mario Draghi in his seminal 2024 report on European competitiveness, "Technological change is accelerating rapidly. Europe largely missed out on the digital revolution led by the internet and the productivity gains it brought: in fact, the productivity gap between the EU and the US is largely explained by the tech sector [...] With the world on the cusp of an AI revolution, Europe cannot afford to remain stuck in the "middle technologies and industries" of the previous century. We must unlock our innovative potential.[21]"

If national security concerns tend to crystallize around continuity of operations in times of crisis, economic security concerns are usually more structural as they center on whether a country (and its domestic firms) can compete, scale, and innovate in markets where the key "chokepoints" are controlled by a small number of gatekeepers such as hyperscalers, dominant platforms, and frontier-model providers.

Middle-power countries are vulnerable at multiple points of the technology stack: from access to high-value datasets and the rules that govern their portability and reuse, to access to high-performance computing resources and cloud environments, and increasingly to access to (and control over) frontier foundation models and their surrounding ecosystems. For middle powers Widespread public and private reliance on foreign hyperscalers and hardware providers creates increasingly alarming dependencies and vulnerabilities. The German country report, for instance, notes that the reduction of structural dependencies on non-EU cloud and technology providers is a central driver of its approach to technological sovereignty.

This economic-security lens also explains why "sovereignty" debates now frequently distinguish research strength from commercialization power. Several jurisdictions report world-class R&D capacity but face constraints in translating that into globally scaled products—constraints that are often amplified by platform concentration. Canada, for example, is acknowledged as a global leader in fundamental AI research, but is struggling to turn research into products ready for commercialization at scale[22]. The French country report highlights a related problem: even where domestic successes exist, the tech ecosystem remains constrained by underinvestment in the physical layers (chips, GPUs, hyperscale facilities) and by dependence on foreign technologies and capital. In practice, when late-stage scale-up capital is thinner at home, promising domestic firms can become dependent on foreign financing, infrastructure partnerships, and distribution channels and such dependencies may later translate into loss of strategic control (through acquisition, foreign influence, or relocation of core assets).

These same dynamics underpin a second economic-security threat: coercive trade or sanctions pressure that disrupts access to hardware, software, capital, or markets, thereby shaping domestic policy choices even absent formal "interference." The mechanism is not always a direct legal prohibition; it can operate through uncertainty, compliance risk, and the commercial risk appetite of global suppliers. Where a country's economy is deeply integrated with a dominant partner, the political salience of this constraint rises quickly. For example, Canada's changing strategic posture is framed in unusually direct terms, including Prime Minister Mark Carney's statement in March 2025 that **Canada's old relationship with the United States"based on deepening integration of our economies and tight security and military cooperation (...) is over."**

The core point for technological autonomy is that a concentrated external dependency converts trade friction into a technology constraint, because modern trade measures often reach deep into the technology supply chain: semiconductors, GPUs, cloud credits, cyber tooling, and export-controlled components.

17 Christian D. Orr, "F-35 vs. JAS 39 Gripen Fighter Debate In Canada Might Already Be Decided", *National Security Journal*, 6 December 2025, available online: https://nationalsecurityjournal org/ f-35-vs-jas-39-gripen-fighter-debate-in-canada-might-already-be-decided/

18 Military Watch Magazine, "Why German Policymakers Are Concerned an American 'Kill Switch' Could Disable Their F-35 Fleet", *Military Watch Magazine*, 9 March 2025, available online: Why German Policymakers Are Concerned an American 'Kill Switch' Could Disable Their F-35 Fleet

19 Military Watch Magazine, "Why German Policymakers Are Concerned an American 'Kill Switch' Could Disable Their F-35 Fleet", *Military Watch Magazine*, 9 March 2025, available online: https://nationalsecurityjournal.org/forget-the-kill-switch-how-america-really-controls-the-f-35-stealth-fighter/

20 Cedric Solidon, "The Word is Out: Danish Ministry Drops Microsoft, Goes Open Source", *Tech Report*, 11 June 2025, available online: https://techreport.com/news/business/denmark-drops-microsoft/

21 Mario Draghi, *The Future of European Competitiveness: Part A — A Competitiveness Strategy for Europe*, Publications Office of the European Union, September 2024, available online: Draghi Report 2024: The future of European competitiveness – European Commission

22 On the other hand, Argentina shows how difficult this can be when structural constraints persist: with R&D spending stuck around 0.5% of GDP and limited scientific infrastructure, progress has been slow despite plans to raise investment.

Finally, middle-power countries increasingly treat incursions on domestic policy space as an economic-security threat: not only through trade negotiation leverage, but also through platform rule-setting (terms of service, app store governance, algorithmic ranking rules, developer access terms) and sustained lobbying pressure in environments where local infrastructure and capital are thin. The Swiss county report provides a concrete illustration of this category, noting lobbying by foreign tech companies during the revision of Swiss data protection law (FADP) with a view to influencing cross-border transfer provisions. At the EU level, implications of the European Commission's Digital Omnibus Package (which would, among other things, revise certain provisions of the EU AI Act) are ambiguous, as they are perceived both as a legitimate simplification initiative affecting digital regulations aimed at a "clearer, simpler, and more innovation-friendly" application of the AI Act and as an example of the impact of foreign incursions on domestic policy priorities.

The unifying economic-security lesson is that, in technology markets characterized by scale economics and network effects, "dependency" is not just a procurement issue—it is a market-structure issue. Gatekeepers can set the price and terms of access (to distribution, data, and compute), while concentrated external dependencies can translate geopolitical pressure into domestic industrial outcomes (who can build, who can scale, and where value accrues). Middle powers' technological sovereignty agendas therefore increasingly blend competition and platform tools with industrial policy and capacity-building: not to pursue autarky, but to keep markets contestable and to ensure that domestic firms and public institutions retain credible options when the terms of access become strategically or economically unfavorable.

3 - Fundamental Values

A third technological sovereignty threat category concerns threats to fundamental democratic values: privacy, due process, equality before the law, and public trust in state institutions. Here, the core issue is not simply that data may be accessed by a foreign authority, but that access may occur through an extraterritorial legal regime that bypasses and contradicts local judicial safeguards, undermining the credibility of domestic fundamental rights frameworks. This is why **"data residency is not data sovereignty"** has become a central refrain. Recognizing these risks, Argentina introduced a 2025 legislative bill on mandatory data localization, aiming to prevent opaque compliance pathways that undermine domestic legal safeguards and public trust. The Government of Canada's public cloud white paper makes the point in plain terms: "Regardless of where the cloud resources are physically located, when data is stored in a cloud environment, the stored data may be subject to the laws of other countries," including the possibility that a provider "could be required to comply with a warrant, court order or subpoena request from a foreign law enforcement agency," potentially even "without notice."[23] In other words, "keeping the bits in-country" can mitigate some operational risks, but it does not necessarily restore exclusive legal control.

A legal opinion prepared in March 2025 for the German Federal Ministry of the Interior sharpens this concern further by exploring in detail the extent to which US law authorizes US government and regulatory authorities to gain access to data held abroad[24]. It concludes that U.S. authorities have "wide-ranging" access and disclosure powers over communications data and cloud-stored information, with meaningful reach even where servers are located outside the United States, subject only to limited remedies for European entities[25]. The opinion distinguishes between access mechanisms used by intelligence authorities, most notably pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA)[26] and Executive Order 12333[27]; and law-enforcement access mechanisms under Sections 2701–2713 of the Stored Communications Act (SCA)[28], as amended by the CLOUD Act[29]. The opinion stresses that Section 702 applies broadly to cloud computing providers and data centers, and that disclosure under Section 702 proceeds largely without publicly transparent judicial review, with the Foreign Intelligence Surveillance Court (FISC) involved primarily through an annual certification framework rather than individualized warrants. Executive Order 12333 is described as providing a basis for intelligence collection from servers abroad without the cooperation of cloud providers, including by exploiting vulnerabilities in IT infrastructure. This architecture is precisely what makes the "fundamental values" issue acute: the operative safeguard is not whether a dataset is hosted in Berlin, Dublin, or Montreal, but whether a provider (or its corporate group), which has effective control over the infrastructure and the data, is subject to legal compulsion, secrecy obligations, and technical compliance pathways under a foreign intelligence regime.

This is also where the sovereignty debate often turns to a second proposition: even "domestic" providers may not be fully insulated if they have sufficient operational presence in the United States. In a modern cloud context, the CLOUD Act and related U.S. legal processes focus on whether a provider is subject to U.S. jurisdiction and has "custody, control, or possession" over the data, and the practical question becomes the degree of U.S. presence and control within the corporate structure[30].

The legitimacy challenge for governments is that public trust is more easily maintained where foreign access routes through domestic legal processes and oversight, rather than through opaque or unilateral pathways. As middle powers increasingly use cloud capacity and AI solutions in sensitive domains, this is increasingly a values issue as much as a security issue: if citizens believe their data can be accessed under foreign authorities' rules without meaningful local constraint confidence in digital government, cross-border data flows, and rights-respecting innovation, and ultimately in their own governments, may erode even where no abuse is proven.

23 Treasury Board of Canada Secretariat, *Government of Canada White Paper: Data Sovereignty and Public Cloud*, Government of Canada, available online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html

24 University of Cologne, Faculty of Law, *Rechtsgutachten zur US-Rechtslage zum weltweiten Datenzugriff durch US-Behörden bei Nutzung von Cloud-Diensten*, University of Cologne, March 2025
25 Ibid
26 Andreas Kuersten, *Foreign Intelligence Surveillance Act (FISA)*, Congressional Research Service, 17 December 2024
27 National Security Agency / Central Security Service, "Executive Order 12333", *NSA.gov*, National Security Agency / Central Security Service
28 Legal Information Institute, Cornell Law School, "18 *U.S. Code* Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access", U.S. Code, Legal Information Institute, Cornell Law School
29 U.S. Congress, Senate, S.2383 - *CLOUD Act, 115th Congress (2017-2018)*, Congress.gov, Library of Congress, 6 February 2018
30 Joe Castaldo and Pippa Norman, "Canada wants to detangle its data from U.S. tech giants. Can it be done?", *The Globe and Mail*, 17 October 2025

Part 2

Legal and Policy Responses to Threats to Technological Sovereignty

1 - The EU is not alone: a converging alignment on a nuanced definition of technological sovereignty

Although the Draghi report has helped crystallize technological sovereignty as a central project of the European Union, the annexed country reports show that the same agenda is now equally salient across a wider set of "middle power" countries with broadly aligned democratic values and overlapping economic and national security interests.

As described in the annexed German country report, the core driver for technological sovereignty is to reduce structural dependence on non-EU hyperscalers and associated exposure to non-EU jurisdiction, pursued through interlocking strategies (including sovereign cloud and public-sector multi-cloud initiatives) rather than a single sovereignty statute. France similarly treats sovereignty as a major political priority, operationalizing it through trusted-cloud certification and public-sector segmentation for sensitive workloads. Italy's approach is explicitly structured around public-sector data classification, cloud certification, and the creation of a national strategic hub to host critical and strategic public data in a way that mitigates non-EU jurisdictional risk.

But the same conceptual frame is visible beyond the EU. The Norwegian country report expresses the same concept as "actual technical and legal" national control over critical ICT assets. Switzerland, while less overtly "sovereignty-first" in its posture, frames cloud strategy and future regulatory development as tools for reinforcing domestic control over key technologies and infrastructure, and does so without adopting an autarkic model.

In short, as described in the annexed country reports, many middle power countries are converging on a pragmatic definition of technological sovereignty: governments are not pursuing autarky, but are trying to preserve credible freedom of action in sensitive domains (public administration, defence, critical infrastructure, health and high-impact AI) while keeping the broader economy open and interoperable.

2 - Data Protection and Lawful Access: data residency is not data sovereignty

Across middle-power countries, the privacy/data security/lawful access dimension functions as the "values backbone" of technological sovereignty: the same dependencies that create economic and national security vulnerability, such as reliance on foreign hyperscalers for datasets, high-performance compute, and increasingly the access layer around frontier models, also create a persistent concern that data may be exposed to foreign actors, accessed without locally acceptable due process, or become unavailable at the moment of greatest sensitivity. Such concerns were expressly brought to the fore in the seminal Schrems decisions in the EU[31].

31 Court of Justice of the European Union, *Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559*, EUR-Lex, 16 July 2020, available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311

This is why, as shown in the annexed country reports, middle powers deploy sovereignty controls not only in the form of industrial policy slogans but as concrete legal and governance responses across four adjacent regimes: data ownership and exclusivity rights, privacy and cross-border transfer law, critical infrastructure security obligations, and lawful access constraints.

The most visible and widely used policy lever to help ensure the protection of nationally sensitive data is public-sector cloud governance, because it sits at the intersection of national security, economic resilience, and fundamental values. France and Italy exemplify an approach that combines data/workload classification by sensitivity, security certification or trusted-cloud standards, and procurement channels that steer the most sensitive workloads into environments designed to reduce exposure to third-country jurisdiction risk and to improve auditability and continuity. Germany and the UK present a more explicitly "risk-managed" posture, but still rely heavily on diversification (multi-cloud), sovereign or government-operated cloud components, and stricter controls for defence and high-value government data in practice. Canada's approach similarly accepts controlled use of commercial public cloud for defined classes of government information, while emphasizing stronger contractual and continuity protections (data access/disclosure clauses, business continuity, disaster recovery planning, vendor-neutral formats and encryption practices) as core sovereignty mitigations.

The country reports converge on a tiered operating model for "secure instances" that accepts that the highest-sensitivity workloads often require architectures that are deliberately less convenient but more controllable. Canada's framework recognizes a government classification system (Protected vs. Classified) and treats higher-sensitivity data as generally incompatible with routine public cloud use. France's SecNumCloud[32] model and Italy's PSN similarly represent an institutional choice to create "trusted/sovereign" lanes for sensitive public workloads and data. At the extreme end, organizations revert to on-premises, restricted tenancy, or even air-gapped deployments for national security, defence, and other truly high-consequence datasets. The policy significance is that these are not merely rare exceptions; they are starting to become the default policies[33] for safeguarding fundamental values where hyperscaler dependency and extraterritorial access risk combine to create dependency risks. The practical effect across jurisdictions is a growing pattern of "functional localization" for sensitive public-sector and regulated datasets, even where the black-letter law remains permissive for general commercial transfers. Recognizing that data residency does not equate to data sovereignty, the country reports consistently note recent investments in "sovereign compute" capacity.

A second shared response is to use data protection/privacy regimes not as blanket data residency mandates (which are often politically and economically costly), but as governance mechanisms that increase friction and accountability for cross-border transfers, particularly where foreign lawful access or surveillance risk is salient. **In short, borders appear to be thickening in relation to cross-border data transfers.**

EU jurisdictions rely on GDPR Chapter V mechanisms[34], including adequacy decisions, Standard Contractual Clauses, Binding Corporate Rules, and post-Schrems transfer impact assessments, as the core legal constraints on cross-border flows. Argentina has taken the GDPR as a model and has implemented Standard Contractual Clauses, Binding Corporate Rules, and express consent requirements for cross-border data transfers to jurisdictions that do not provide an adequate level of protection, as determined by the Argentine Data Protection Authority. Italy additionally describes a practical "de facto localization" trend driven by transfer compliance scrutiny rather than formal bans. Canada also imposes continuing responsibility for comparable protection when personal information is transferred for the transferor, and (in Québec) a prior privacy impact assessment requirement before communicating personal information outside Québec. Across these jurisdictions, the policy posture is consistent: cross-border data movement remains legally possible, but only under conditions that preserve a level of protection and redress that domestic publics perceive as legitimate and that can be defended politically when foreign lawful access risks are raised.

Enforcement posture reinforces the point that these are not theoretical sovereignty concerns. Canada's privacy commissioners for instance faulted TikTok for failing to obtain meaningful consent where cross-border transfers were at issue, underscoring that regulators are prepared to treat cross-border data practices as an active compliance obligation. The broader implication is that "sovereignty" is increasingly operationalized through legal enforcement: organizations cannot rely on contractual boilerplate or generic transparency language if transfer realities or platform architectures create heightened extraterritorial exposure.

On lawful access, the common design principle is that ordinary state access should be anchored in judicial oversight and particularity (rejecting bulk or indiscriminate collection as a routine model), while exceptional intelligence collection is treated as a distinct, specially governed framework. The country reports treat foreign lawful access risk as a key driver of sovereignty initiatives — Canada notes renewed attention to U.S. lawful access concerns in the context of dependence on foreign hyperscalers, while Germany's debate is explicitly animated by reliance on U.S. hyperscalers and potential exposure to U.S. lawful-access regimes. In terms of "blocking-statute style" constraints, the practical analogue across jurisdictions is the insistence that foreign access requests, where they are to be honored, should be channeled through recognized cooperation mechanisms (MLAT/e-evidence type instruments) rather than unilateral extraterritorial compulsion. Canada's mutual legal assistance framework exemplifies this due-process channel: court-ordered assistance is available under the Mutual Legal Assistance in Criminal Matters Act[35] for treaty partners, and requires reasonable grounds and a clear connection between the foreign investigation and evidence in Canada.

32 Agence nationale de la sécurité des systèmes d'information (ANSSI), "Cloud", *ANSSI*, French Government, available online: https://cyber.gouv.fr/enjeux-technologiques/cloud/

33 Treasury Board of Canada Secretariat, *Government of Canada White Paper: Data Sovereignty and Public Cloud*, Government of Canada, available online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html ; see also Global Affairs Canada, "Notice to exporters no. 1159 — Guidance on the movement to and storage of controlled technology in the Cloud", Canada.ca, Government of Canada, 5 November 2025, available online: https://www.international.gc.ca/trade-commerce/controls-controles/notices-avis/1159.aspx?lang=eng

34 General Data Protection Regulation (GDPR), April 2016, available online: https://gdpr.algolia.com/

35 Department of Justice Canada, *Mutual Legal Assistance in Criminal Matters Act, R.S.C., 1985, c. 30 (4th Supp.)*, Justice Laws Website, Government of Canada, available online: https://laws-lois.justice.gc.ca/eng/acts/m-13.6/index.html

Critical infrastructure security frameworks then sit on top of the privacy/lawful access layer as the resilience and continuity overlay: they treat cybersecurity, supplier concentration, and service continuity as statutory risk-management duties. Italy describes a combination of EU frameworks (including NIS2[36]) and a national cybersecurity perimeter that includes supplier-vetting and incident-notification obligations, explicitly aimed at protecting strategic sectors from cyber threats and supply-chain weakness. The UK similarly links risk management and continuity expectations to the classification of data centres as critical national infrastructure under its NIS regime. Indeed, critical national infrastructure providers have now got to take geopolitics into account when drawing up cyber defence plans. The effect is to translate sovereignty anxiety into board-level and operational controls: mapping dependencies, setting minimum security baselines, and planning for disruption.

3 - AI and Copyright: the challenge of balancing creator rights and innovationy

Large language models require massive quantities of training data, and the legality of acquiring and using that data is now a central fault line in technology policy. What is emerging is not simply a technical debate about model performance, but a sustained legal and political dispute about the boundary between lawful reuse and misappropriation. This forces jurisdictions to reconcile two powerful but competing objectives:

- maintaining a strong copyright framework that preserves incentives for authors, creators, and rightsholders;
- and enabling transformative innovation that, in practice, often depends on broad access to cultural products.

Because copyright is anchored in the Berne Convention and related instruments, this debate is especially complex: governments are trying to re-balance domestic innovation incentives without destabilizing a highly harmonized international baseline.

The issue has spawned not only a huge amount of (as yet largely mostly unsettled) litigation[37], but also a series of (still pending) attempts at copyright law reform[38].

The annexed country reports illustrate that jurisdictions are approaching the "training data problem" through different doctrinal paths, and that those choices have technological sovereignty consequences in both directions. Canada is a useful illustration of the "fair dealing" model: the report characterizes Canadian fair dealing as a closed, exception-based system, and notes concerns that this narrower approach can make unlicensed "screen scraping" for model development more legally risky in Canada than in jurisdictions that have broader, principle-based "fair use" exceptions. In contrast, a number of European countries (and the UK, in a more limited way) are navigating through explicit TDM exceptions rather than relying on a general fair use doctrine. The implementation of TDM exceptions (including for scientific research) in Germany and Italy, for instance, may reduce transaction costs and provide clearer legal footing for certain classes of training activity. Argentina represents the most restrictive end of this spectrum: it lacks both a principle-based fair use doctrine and explicit TDM exceptions, relying instead on closed copyright exceptions, which significantly increases legal uncertainty for unlicensed data use in AI training and reinforces reliance on foreign-trained models.

From a technological sovereignty perspective, these different approaches cut both ways. A more restrictive approach may reduce the attractiveness of a jurisdiction as a site for frontier model training and related investment, particularly where compute and capital are mobile, thereby potentially weakening domestic capability and increasing reliance on foreign model providers. Conversely, an overly permissive regime may undermine the economic incentives that sustain domestic cultural industries and professional creation, with downstream sovereignty costs of a different kind: erosion of national creative ecosystems, bargaining power, and the legitimacy of the innovation model in the eyes of the public. In this sense, "sovereignty" is not only about domestic compute and data control; it is also about preserving a credible social contract around human creation and expression, while acknowledging that generative AI can also enable new forms of creativity and new markets. The hard policy reality, reflected across the reports, is that there is no frictionless solution: whichever doctrinal route a jurisdiction prefers, fair use, fair dealing, or TDM exceptions, it is implicitly choosing a distribution of costs and benefits between creators, model developers, downstream users, and the state's broader strategic autonomy goals.

36 European Commission, "NIS2 Directive: securing network and information systems", *Shaping Europe's Digital Future*, European Commission, 20 January 2026, available online: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive NIS2 Directive: securing network and information systems

37 See e.g. United States District Court for the Northern District of California, *Richard Kadrey et al. v. Meta Platforms, Inc., Case No. 23-cv-03417-VC, Order Denying the Plaintiffs' Motion for Partial Summary Judgment and Granting Meta's Cross-Motion for Partial Summary Judgment*, 25 June 2025

38 See e.g.: Innovation, Science and Economic Development Canada, *Consultation on Copyright in the Age of Generative Artificial Intelligence: What We Heard Report*, Government of Canada, 2025, available online: https://ised-isde.canada.ca/site/strategic-policy-sector/en/marketplace-framework-policy/consultation-copyright-age-generative-artificial-intelligence-what-we-heard-report#s1 and Intellectual Property Office, *Copyright and AI: Consultation*, Intellectual Property Office, December 2024

4 - Procurement/Competition and Trade Policy: balancing the protection of open markets with the need to encourage domestic champions

Economic and industrial policy responses to technological sovereignty, as summarized in the country reports, are best understood as an effort to shift from reactive "risk mitigation" to proactive "capability shaping," using three levers in combination: competition tools to keep markets contestable, procurement to create dependable demand and reduce lock-in, and fiscal measures (tax incentives and targeted funding) to close the compute-and-commercialization gap that leaves middle powers structurally dependent on foreign incumbents.

The German country report, for example, explicitly links sovereignty threats to platform concentration and foreign hyperscaler dependence and treats competition enforcement as part of the response to gatekeeper power and dependency. France and Italy complement competition policy with procurement and certification-based measures that reduce switching friction and reinforce interoperability. France's cloud framework includes rules targeting migration/transfer fees, limiting cloud credits, and imposing interoperability obligations, while Italy's public-sector cloud strategy uses classification and certification to steer sensitive workloads and data toward sovereign or EU-controlled environments. Even jurisdictions that do not embrace overt "buy local" rules (often constrained by trade commitments) still use security carve-outs, qualification requirements, diversification mandates, and strategic screening powers to protect sensitive sectors; Italy, for instance, notes the use of national security tools (golden power) in relation to sensitive network infrastructure choices. Switzerland illustrates the other end of the spectrum: procurement is formally grounded in non-discrimination and transparency aligned with WTO GPA principles, but can still incorporate sustainability/innovation criteria that indirectly shape supplier outcomes.

A key insight running through these approaches is that procurement demand can be more decisive than subsidies, because anchor-customer revenue de-risks scaling and can create a domestic "market pull" for sovereign offerings (compute, cloud controls, cybersecurity, and sector-specific AI). Canada's country report reflects this orientation in its emphasis on procurement and contractual controls as sovereignty tools, strengthening clauses on data access/disclosure and business continuity, and building resilience against disruption or deplatforming. In Canada, technological sovereignty is also situated within a broader economic integration strategy, including legislative moves designed to remove internal barriers and accelerate "projects in the national interest"[39] in the name of prosperity, national security, and national autonomy. Against that backdrop, the types of initiatives you flag (public–private arrangements to secure GPU supply and model capacity; "AI factories" and domestic compute build-outs; pension-fund interest in HPC/data centre assets) align with the broader middle-power playbook: use public procurement and long-duration capital to expand local compute supply while the legal risk questions (especially lawful access exposure and jurisdictional control) become part of diligence and valuation, not merely compliance.

The country reports also point to the need for a more precise answer to the question "how much compute power is enough?" Because unconstrained scaling can create environmental and governance externalities (and may ultimately be wasteful or misguided[40]), this suggest adopting a AI compute sovereignty model that values not only raw capacity but fit-for-purpose deployment (e.g., smaller, focused models for more narrowly defined use cases of demonstrable public or private benefit) alongside guardrails and safeguards that reinforce democratic values and reduce waste.

The trade dimension is increasingly framed as "integration as resilience." The Canadian report explicitly describes a strategic reorientation away from reliance on a single partner and toward diversifying trade relationships, combined with internal market strengthening and faster delivery of strategic projects[41]. In parallel, the EU-facing jurisdictions emphasize that sovereignty is not a purely national project but a coordinated one. The emerging opportunity for middle powers is therefore twofold: reduce fragmentation at home (e.g., internal market barriers) while deepening trusted trade and regulatory alignment with like-minded partners—so that supply chains, compute access, and investment channels become more resilient without retreating into autarky.

Across competition law and platform policy, the reports treat market contestability and lock-in reduction as an economic-security component of technological sovereignty. The German report is explicit that platform concentration and foreign dependency risks are addressed in part through competition enforcement tools alongside EU-level initiatives.

Procurement rules and trade commitmenwwts operate as both constraint and tool. Most jurisdictions cannot (and do not) rely on overt "buy local" mandates, given trade commitments; instead they use national security carve-outs, qualification/certification requirements, supplier diversification, and investment-screening or "golden power" style tools[42] to protect strategic sectors and shape outcomes through project-level conditions. Italy is explicit that there is no general buy-local requirement, but national security tools are used to protect strategic infrastructure choices. Switzerland similarly notes the absence of explicit "buy Swiss" rules, while leaving room for sustainability and innovation criteria that can indirectly influence supplier selection.

39 Government of Canada, "Building Canada Act – Projects of National Interest", *One Canadian Economy*, Canada.ca, 2025, available online: https://www.canada.ca/en/one-canadian-economy/services/building-canada-act-projects-national-interest.html

40 PYMNTS, "Meta Chief AI Scientist Slams Quest for Human-Level Intelligence", *PYMNTS*, 8 January 2025, available online: https://www.pymnts.com/artificial-intelligence-2/2025/meta-large-language-models-will-not-get-to-human-level-intelligence/

41 Parliament of Canada, *Bill C-5, One Canadian Economy Act, 1st Session, 45th Parliament, 3 Charles III, 2025, Statutes of Canada 2025, c.* 2, Parliament of Canada, 26 June 2025, available online: https://www.parl.ca/DocumentViewer/en/45-1/bill/C-5/royal-assenthtml

42 Department for European Affairs, Presidency of the Council of Ministers, "Golden power", *Europarole*, Italian Government, 20 June 2023, available online: https://www.affarieuropei.gov.it/it/comunicazione/europarole/golden-power/

Finally, most jurisdictions pair these regulatory and procurement levers with targeted fiscal and industrial measures, tax incentives, R&D subsidies, and strategic compute investments, to build endogenous capacity in the layers that matter for autonomy (compute, cybersecurity, sovereign cloud components, AI research translation). Canada points to major public commitments toward sovereign AI compute capacity, but also notes the challenge of competing with the scale of foreign private investment. France anchors its sovereignty agenda in large-scale investment programs (France Relance/France 2030)[43] that explicitly pursue industrial and technological autonomy, including cloud acceleration. Switzerland's patent box and R&D super-deduction illustrate a more tax-structural approach tied to domestic R&D substance and IP linkage.

Overall, the combined picture is a "portfolio strategy" which starts by defining technological sovereignty as controlled autonomy rather than isolation. Within this context, specific legal and policy measures are adopted including segmenting data and workloads by sensitivity; steering the most sensitive to trusted or sovereign environments via procurement and certification; hardening continuity requirements and supplier-risk management through cybersecurity and contracting; using privacy and transfer governance to mitigate cross-border transfer risks; using competition laws and procurement rules to reduce lock-in; and using tax/funding instruments to close the commercialization and infrastructure gap that otherwise leaves sovereignty as a paper policy rather than a reality that can be acted upon.

43 French Government, "Understanding France 2030", *France 2030*, info.gouv.fr, 7 May 2024, available online: https://www.info.gouv.fr/grand-dossier/france-2030-en/understanding-france-2030

Technological Sovereignty Country Reports

Argentina

Diego Fernandez, Marval, O'Farrell & Mairal, Buenos Aires

Argentina's technological autonomy is shaped by structural constraints and significant, though uneven, strategic strengths. Underinvestment in Research & Development (R&D) – around 0.5% of Gross Domestic Product "GDP") – and limited scientific infrastructure have slowed innovation despite recent efforts to raise R&D investment to 1.7% of GDP by 2030. The country remains highly dependent on foreign technological inputs, imports most advanced hardware and critical equipment, and suffers from a technological trade deficit. This external reliance exacerbates the region's digital divide and weakens Argentina's digital sovereignty.

Argentina has achieved genuine reasonable technological sovereignty in nuclear and space technologies through sustained state policies, placing the country among a small group with advanced capacities in satellite development, nuclear reactors, and biotechnology. These strengths contrast with certain vulnerabilities in electronics, advanced computing, and high-end manufacturing, where local production remains limited.

Several external threats compromise national autonomy, including dependence on multinational suppliers, exposure to foreign commercial and geopolitical pressures, and the influence of global norms and standards shaped by major powers or big tech companies. Decisions by foreign actors -such as supply restrictions or unilateral service limitations- can directly affect communications, data flows, and access to critical technologies.

Despite these challenges, Argentina has demonstrated success in key sectors that underpin sovereignty. The country maintains internationally recognized capabilities in nuclear energy, has developed national satellite systems (ARSAT, SAOCOM), and has built a strong bioeconomy with notable achievements in agricultural biotechnology and vaccine production. Emerging AI ecosystems, although still small, reveal growing domestic expertise and an intention to develop digital tools tailored to national needs.

Active public policies reinforce autonomy in defense, health, agriculture, energy, education, and cybersecurity. These include local production of military systems and drones, national vaccine manufacturing, precision agriculture technologies, renewable-energy capacity development, digital inclusion programs, and a National Cybersecurity Strategy focused on building domestic capabilities.

Looking ahead, Argentina identifies a set of strategic technologies essential for future autonomy: artificial intelligence, big data, quantum computing, biotechnology, satellite and space systems, nanotechnology, robotics, additive manufacturing, and Industry 4.0 technologies. Developing local capacities in these fields is considered crucial to reduce external dependency, strengthen sovereignty, and positioning the country competitively in the global knowledge economy.

Canada

Charles Morgan, McCarthy Tétrault LLP, Montreal
Francis Langlois, McCarthy Tétrault LLP, Montreal

Few countries in the world are as economically integrated as the United States and Canada. In 2024, Canada was the largest importer of US goods in the world and the US's third largest source of imported goods (after China and Mexico). Nevertheless, in the context of the current US government's dramatic recent shifts in trade and military policy, Canada has had to radically reassess this relationship and its implications for Canada's resilience and autonomy. Canadian Prime Minister Mark Carney stated in March 2025 that Canada's old relationship with the United States, "based on deepening integration of our economies and tight security and military cooperation, is over".

Canada's new economic reality has brought with it a heightened awareness of its fundamentally unhealthy reliance on a single economic partner and a new resolve to increase its economic, technological and military autonomy. In particular, Canada has begun to focus increasingly on the removal of internal trade barriers (as between provinces) and to increase trade with partners in both Asia and Europe, in the hope that increased "East-West" trade will offset losses in "North-South" trade with the aim of doubling non-US exports over the next decade.

In this context, one of the very first acts of the newly elected Carney government was to adopt "An Act to enact the Free Trade and Labour Mobility in Canada Act and the Building Canada Act". Part 1 of the act establishes a statutory framework to remove federal barriers to the interprovincial trade of goods and services and to improve labour mobility within Canada. Part 2, referred to as the "Building Canada Act" is designed to "enhance Canada's prosperity, national security, economic security, national defence and national autonomy by ensuring that projects that are in the national interest are advanced through an accelerated regulatory process. Canada has also aggressively pursued new free trade deals, including with Indonesia.

In this context, technological sovereignty has become a matter of particularly focused concern in Canada. Canada is widely acknowledged to be a global leader in fundamental AI research, with multiple world-renowned universities and research centers, supported by the Pan-Canadian Artificial Intelligence Strategy, the world's first national strategy dedicated to AI. Although those capacities have helped Canada play a key role in the research and development of AI technologies, Canada has so far struggled in moving research into products and commercialization, with certain notable exceptions like foundational models provider Cohere.

Canada is also generally dependent on foreign hyperscalers for cloud hosting and AI compute capacity, which has led to renewed concerns related to foreign companies and foreign governments having access to Canadian data. Revisiting themes and concerns that had initially first been raised (and largely resolved) following the adoption of the USA PATRIOT Act in 2001, the Canadian government and many private sector enterprises are currently re-examining the implications and perceived risks associated with the U.S. CLOUD Act of 2018.

In this context, Canada has appointed its first federal Minister of Artificial Intelligence and Digital Innovation, Evan Solomon, with a mandate to boost AI adoption, increase trust in AI, and build sovereign AI architecture. In October 2025, the Canadian Federal government published a framework to promote digital sovereignty, defined as "the ability of the [Government of Canada] to exercise autonomy over its digital infrastructure, data and intellectual property". Amplifying an international trend to promoting "thicker borders" as regards trans-border data transfers of sensitive data, the framework acknowledged that storing data in Canada or with Canadian service providers does not in itself guarantee data will be outside the jurisdiction of foreign courts and stated that the Government of Canada ("GC") "can fully maintain legal control only when it delivers services itself or works with providers that operate entirely under Canadian jurisdiction".

Recent federal budgets have included investments underscoring commitments to strengthen Canada's technological infrastructures, including the "Canadian Sovereign AI Compute Strategy" (2024) with $2 billion earmarked until 2030 to develop domestic high-performance computing for AI. Likewise, Canada's National Quantum Strategy (2023) dedicates $360 million to quantum research, talent, and commercialization, aiming to solidify Canada's leadership in quantum technologies. Those investments remain however modest when compared against investments by leading foreign private tech firms.

Acknowledging that an overly prescriptive "fair dealing" regime under Canada's Copyright Act may discourage homegrown efforts to train AI models in Canada, the Government of Canada conducted a Consultation on Copyright in the Age of Generative Artificial Intelligence between October 12, 2023, and January 15, 2024, to better understand the effects of generative artificial intelligence (AI) on copyright and the marketplace. The results of the consultation have so far been inconclusive and no amendments to the Copyright Act have yet been adopted.

Although AI, advanced computing, cloud and 5G networks are currently the main focus of Canadian technology autonomy policy and efforts, the Carney government has also looked to diversify its military spending to reduce over-reliance on the United States, ordering a review of Canada's plan to purchase a fleet of F-35 fighter jets under an existing deal with Lockheed Martin and the US government, while pursuing negotiations with Swedish defense company Saab and the Canadian aerospace company Bombardier to build the Saab Gripen fighter jet under license in Canada, while potentially turning to German and South Korean suppliers (instead of US suppliers) in relation to an anticipated purchase of new military submarines.

France

Bertrand Cassar, La Poste, Paris
Emmanuelle Mignon, August Debouzy, Paris
Gilles Rouvier , Lawways Avocats, Paris
Mathilde Lécaillon, Lawways Avocats, Paris
Grimaud Valat, Duclos, Thorne, Mollet-Viéville & Associés (DTMV), Paris

The main concerns regarding France's technological autonomy are twofold: on the one hand, threats to cybersecurity and the risk that malicious States could seriously compromise the country's functioning and the satisfaction of its population's basic needs; on the other hand, the growth and investment deficit that prevents France from remaining at the right technological level, if not catching up, and makes it dependent in many areas on foreign technologies and capital.

This dependence is now increasingly visible at the level of core digital infrastructures: a significant share of the large-scale data centres and AI computing facilities being built in France are financed and controlled by non-European investors. At the Paris AI Action Summit in February 2025, President Macron announced around €109 billion of mainly private investment in AI, including up to €50 billion from the United Arab Emirates for a 1-gigawatt AI campus and €20 billion from the Canadian fund Brookfield for a hyperscale data centre in Cambrai, alongside multi-billion projects by American cloud and colocation providers such as Amazon, Digital Realty and Equinix. France is trying to close its infrastructure gap partly by relying on non-European capital and operators, which further entrenches its vulnerability. Moreover, when French companies do succeed in AI, a substantial share of their equity quickly ends up in the hands of non-European investors: Mistral AI, for instance, has raised several billion euros since 2023 from US venture capital funds such as Lightspeed, Andreessen Horowitz, General Catalyst, Index Ventures and DST Global, as well as global tech players like NVIDIA, and is currently negotiating an additional $1 billion equity round with Abu Dhabi's sovereign fund MGX.

While France has had real industrial successes (Mistral AI in the field of AI, Scaleway in the field of cloud computing, Outscale in the field of sovereign cloud computing, Orange in the field of cybersecurity, FranceConnect for digital identity management), and while it retains the ability to train top-level engineers, these successes alone cannot make up for the lack of private investment, particularly in the areas of servers, telecoms, and chips. Like many European countries, France also faces difficulties in accessing rare earths.

Over the last decade, public policies and private initiatives have largely prioritised software, algorithms and the creation of "European champions" in AI and cybersecurity, while under-investing in the underlying physical layers: semiconductor manufacturing, GPU production, high-capacity data centres and energy-intensive network infrastructure. France is emerging as a producer of code and digital services that rely on hardware, networks and hyperscale facilities that are designed, manufactured or financed abroad, limiting the effective scope of its technological autonomy.

In terms of regulation, France relies on the extensive European legislative arsenal and has also adopted effective national legislation such as the anti-Huawei law and foreign investment controls. However, there is a glaring imbalance between excessive regulation and insufficient private capital, which the State is attempting to address with public subsidies that are not always effective and increase the debt. While there have been attempts to guard against extraterritorial legislation, the real cause of its effectiveness, which is economic, is difficult to address in this context.

Germany

Alexander Tribess, GreenGate Partners Rechtsanwaltsgesellschaft GmbH, Hamburg
Dr. Philip Kempermann, Heuking, Dusseldorf

Germany approaches technological autonomy as a strategic priority that is deeply embedded across its digital, industrial, and innovation policies. Rather than relying on a single framework, Germany pursues technological sovereignty through a series of interlocking national strategies, including the Digital Strategy 2030, multiple cloud and data initiatives, a comprehensive AI strategy, and strong commitments to European cooperation. The country positions technological autonomy as both an economic imperative and a matter of national and European security.

The private sector as well as the government to a large extent makes use of hyperscalers for their technology applications. This creates dependencies on service providers that are under the jurisdiction of non-EU countries. Therefore, a central driver of Germany's approach is the desire to reduce structural dependencies on non-EU cloud and technology providers. This concern informs the Federal Multi-Cloud Strategy, the development of the Deutsche Verwaltungscloud (DVC) for public administration, and Germany's prominent role in GAIA-X and the broader European data and cloud ecosystem. These initiatives are complemented by Germany's open-source strategy, which explicitly promotes open technologies as a means to strengthen sovereignty, security, and interoperability. The political salience of technological autonomy has intensified in recent years, with the federal government openly advocating for European digital sovereignty and embedding this objective in sector-specific policies such as the National Security and Defence Industry Strategy.

Germany's National AI Strategy forms another major pillar of its autonomy agenda. The country has invested heavily in AI research infrastructure, creating six national centres of excellence and supporting the emergence of domestic foundational models such as Aleph Alpha and OpenGPT-X. These efforts are supported by the AI Action Plan 2023 and significant public funding aimed at building an advanced, sovereign AI ecosystem capable of meeting industrial and public-sector needs. In parallel, Germany continues to expand its high-performance computing landscape and its quantum computing capabilities, as seen in major national initiatives such as the DLR Quantum Computing Initiative, the Fraunhofer Quantum Systems Programme, and the Munich Quantum Valley. Collectively, these programmes aim to create domestic capability in cutting-edge compute hardware, algorithms, and applications that underpin long-term autonomy.

Despite these advances, there are several threats to technological autonomy. Germany remains concerned about over-reliance on foreign hyperscalers and exposure to non-EU lawful-access regimes, which reinforces the push for sovereign cloud solutions. Other perceived threats include the global concentration of market power among dominant digital platforms and broader geopolitical dependencies in critical technologies such as semiconductors and telecommunications equipment. These concerns are reflected in Germany's enforcement of competition rules (notably §19a of the German Competition Act) and in the integration of sovereignty objectives into cybersecurity policy under KRITIS and the forthcoming NIS2-based regulatory framework.

At the same time, Germany can point to noteworthy success stories. The most recent big success story is DeepL, the automated translated powerhouse that has changed document translations worldwide and is still independently owned and based in Germany. The launch of the Deutsche Verwaltungscloud in 2025 marks an important milestone for sovereign public-sector IT infrastructure. The country's growing portfolio of quantum computing platforms, such as Quantum System One and QVLS-Q1, demonstrates a commitment to domestic hardware and ecosystem development. Additionally, Germany's leadership in European cloud, data, and AI initiatives positions it as a central architect of Europe's collective technological sovereignty.

Across these developments, several sectors stand out as focal points for implementing technological autonomy policies, including public administration, defence, critical infrastructure, and high-value industrial domains such as automotive, manufacturing, and chemicals. The technologies most closely associated with Germany's autonomy agenda are artificial intelligence, cloud and sovereign data infrastructure, quantum computing, cybersecurity, and open-source software.

Italy

Licia Garotti, Pedersoli Gattai, Milan
Marco Galli, Pedersoli Gattai, Milan

Italy's technological autonomy strategy is strongly aligned with the European Union's broader vision of digital and strategic sovereignty. The country prioritizes reducing dependence on non-EU technology providers, ensuring greater control over critical data, and strengthening resilience in key digital infrastructures. Italy, alongside its national initiatives, embeds its policies within EU regulatory frameworks, which collectively shape the country's approach to data governance, cybersecurity, and safe AI development.

Technological sovereignty is pursued primarily through coordinated European programs, complemented by targeted national measures. Domestically, Italy is enhancing its capabilities in high-performance computing, AI research, and space governance. The national innovation ecosystem is supported by research centers of excellence, expanding compute infrastructure, and tax incentives designed to stimulate R&D and technological innovation.

Regulatory and competition authorities play an increasing role in safeguarding technological independence by scrutinizing data practices, limiting lock-in risks, and ensuring contestable digital markets. Additionally, while Italy has no explicit "buy local" requirements, national security tools help protect strategic sectors from excessive foreign influence.

Overall, Italy is evolving toward a more sovereign and resilient technological framework. Its progress is marked by significant investment in strategic infrastructures, growing attention to data governance and digital risk, and alignment with EU policies that collectively drive the country's long-term goal of reinforcing its technological and industrial autonomy.

Norway

Kristian Foss, Advokatfirmaet Bull AS, Norway

Norway faces a complex landscape in its pursuit of national technological autonomy. A key concern is the country's reliance on foreign-owned cloud and digital platforms, which raises issues of data sovereignty and compliance with strict privacy regulations such as GDPR. Norwegian enterprises often struggle to ensure that sensitive data remains within national borders, particularly when using global cloud providers, creating legal and operational challenges. Additionally, hybrid threats—combining cyberattacks, disinformation, and influence operations—pose risks to Norway's digital infrastructure and public trust, as highlighted by the Norwegian Police Security Service. These vulnerabilities underscore the difficulty of achieving full control over critical technologies and information flows in an interconnected global environment.

Despite these challenges, Norway has notable strengths. The country is among the most digitalized in Europe, supported by world-class infrastructure and high digital literacy. Norway's vibrant startup ecosystem, backed by Innovation Norway and programs like SkatteFUNN, fosters innovation in artificial intelligence, cleantech, and advanced computing. These efforts position Norway as a leader in responsible AI development and as an emerging player in quantum technology, with significant investments announced to strengthen national capacity.

Technological autonomy policies are most visible in sectors critical to national security and competitiveness, including telecommunications, financials, cybersecurity, and green technology. Norway's digitalisation strategy emphasizes secure ICT services, resilient infrastructure, and reduced dependency on foreign providers, aligning with broader European efforts to safeguard digital sovereignty.

The technologies at the center of these policies include artificial intelligence, cloud computing and increasingly quantum technologies. AI governance is being reinforced through the preparations for the implementation of the EU AI Act, while quantum computing and secure communication are prioritized under a dedicated national strategy. In addition, Norway aims to become the world´s most digitalised country by 2030, and will therefore introduce its own law regulating artificial intelligence. This law implements the EU´s AI Act. These focus areas reflect Norway's ambition to maintain competitiveness and security in a rapidly evolving global tech environment.

Switzerland

Nicole Beranek Zanon, Härting Rechsanwälte, Zug
Alesch Staehelin, Uto Legal, Zurich

Switzerland understands “digital / technological sovereignty” in a narrow, state-centred way. The core concern is that the Confederation has sufficient control and ability to act in the digital space to perform its public tasks. The broader role of the private sector and society is addressed mainly within the “Digital Switzerland Strategy,” not as independent holders of “sovereignty.”

Since 11 December 2020, the Federal Administration has pursued a hybrid multi-cloud strategy, allowing a mix of internal and external cloud services from several providers. Digital sovereignty is expressly anchored as a strategic objective in the annually updated Digital Switzerland Strategy, in the Foreign Policy Strategy 2024–2027 and in the “Strategie Digitale Bundesverwaltung,” and has triggered numerous parliamentary initiatives. AI is a priority field: based on the report of 12 February 2025, the Federal Council has adopted a regulatory approach with three goals (innovation, fundamental rights including economic freedom, and trust), intends to implement the Council of Europe AI Convention in Swiss law, and favours sector-specific legislation complemented by limited horizontal rules (especially data protection).

In terms of technological autonomy, Switzerland has strong domestic capabilities but relies heavily on foreign infrastructure in practice. ETH Zurich (including the “Apertus” foundation model and the ETH AI Center) and the ETH Domain more broadly provide substantial AI and quantum-technology know-how and compute.

Public AI funding is significant but routed through general research and innovation instruments (ETH Domain, SNSF, Innosuisse, sector programmes), not through a dedicated “sovereign AI” vehicle, and there is no policy objective of full-stack technological self-sufficiency. Most production-grade AI services still run on non-Swiss cloud providers and non-Swiss base models. AI adoption is high, especially in services and finance, but many organisations are cautious in mission-critical areas because of data-protection, outsourcing and sovereignty risks. Legally, there is no general “data ownership” right, no specific text-and-data-mining exception and no “fair use” clause; copyright limitations are exhaustively listed in Arts. 19–27 URG, and there is not yet case law on unlicensed training of AI models. The revised Federal Act on Data Protection (FADP) distinguishes between personal data, sensitive data and “profiling with high risk,” but does not mandate data localisation.

Cross-border transfers are governed by Art. 16 FADP (adequate protection or appropriate safeguards); derogations apply only narrowly. Information security for critical infrastructures is regulated in particular by the Federal Act on Information Security (ISA), the Ordinance on the Protection of Critical Infrastructures (VSKI), the National Cyber Strategy and Art. 74a FMG, with potential board liability under Art. 754 CO if risk management (including supplier diversification) is insufficient.

Access to data without consent is only permitted under specific statutes and with strict safeguards. Under the Federal Act on the Surveillance of Postal and Telecommunications Traffic (BÜPF / SPTTA), authorities may obtain data from telecom and cloud providers for serious criminal offences only on the basis of prior judicial authorisation; bulk “collect-all” access and warrant-less access are not allowed. Internationally, Switzerland cooperates via the Budapest Convention and MLATs; foreign authorities cannot directly compel Swiss providers, which prevents direct extraterritorial enforcement such as under the US CLOUD Act. Competition and innovation policy support technological autonomy indirectly: the Cartel Act (KG) and the Federal Act on the Promotion of Research and Innovation (RIPA) form the core framework and are applied by COMCO and the Federal Supreme Court (e.g. BGE 143 II 297, Swisscom) to safeguard infrastructure access and innovation dynamics.

Public procurement law is formally non-discriminatory but allows innovation and sustainability criteria; tax law provides a patent box and an R&D super-deduction under the DBG, linked to R&D conducted in Switzerland and to Swiss-related IP. External influences arise in particular from the EU adequacy decision under data protection law and from lobbying by foreign technology firms during the FADP revision, but without formal loss of legislative autonomy. Forthcoming reforms (a Digital Services Act, an AI regulatory framework and a Federal Act on Cybersecurity) are expected to reinforce Switzerland’s regulatory control over key digital technologies.

United Kingdom

Michael Peeters, Addleshaw Goddard LLP, Leeds
Patricia Shaw, Beyond Reach, London

This report examines the United Kingdom's approach to technological sovereignty and autonomy across key regulatory, policy, trade agreements, and other commercial dimensions. The UK's current policy and legislative framework appears to be emphasising economic growth, innovation leadership, and flexible governance rather than defensive data localisation or explicit sovereignty requirements.

The UK (as stands) has no formal definition of 'technological sovereignty' but pursues de facto sovereignty through its National AI Strategy, AI Opportunities Action Plan, the Sovereign AI Unit (established in July 2025), and through significant compute infrastructure investments (£2 billion UK Compute Roadmap) and talent development to ensure the UK is creating its own enablement environment and AI assets. While cloud sovereignty policies remain permissive for the private sector, sensitive government and defence data increasingly stays onshore. This may not be the case for health data held within the NHS.

The UK maintains strong research capabilities through the Alan Turing Institute, AI Security Institute, National Quantum Computing Centre, and National Cyber Security Centre, but remains heavily dependent on US hyperscalers and Asian semiconductor supply chains.

On the whole there appears to be nothing specific in terms of law reform or anticipated regulatory landscape to enforce or endorse technological autonomy for the UK.

For the sake of brevity, we have included only the "executive summary" of each of the eight country reports. The full versions of each country report are available via the QR code below.

Annex A -Technological Sovereignty Country Reports

Argentina

Diego Fernandez, Marval, O'Farrell & Mairal, Buenos Aires

Executive summary

Argentina's technological autonomy is shaped by structural constraints and significant, though uneven, strategic strengths. Underinvestment in Research & Development (R&D) – around 0.5% of Gross Domestic Product "GDP") – and limited scientific infrastructure have slowed innovation despite recent efforts to raise R&D investment to 1.7% of GDP by 2030. The country remains highly dependent on foreign technological inputs, imports most advanced hardware and critical equipment, and suffers from a technological trade deficit. This external reliance exacerbates the region's digital divide and weakens Argentina's digital sovereignty.

Argentina has achieved genuine reasonable technological sovereignty in nuclear and space technologies through sustained state policies, placing the country among a small group with advanced capacities in satellite development, nuclear reactors, and biotechnology. These strengths contrast with certain vulnerabilities in electronics, advanced computing, and high-end manufacturing, where local production remains limited.

Several external threats compromise national autonomy, including dependence on multinational suppliers, exposure to foreign commercial and geopolitical pressures, and the influence of global norms and standards shaped by major powers or big tech companies. Decisions by foreign actors -such as supply restrictions or unilateral service limitations- can directly affect communications, data flows, and access to critical technologies.

Despite these challenges, Argentina has demonstrated success in key sectors that underpin sovereignty. The country maintains internationally recognized capabilities in nuclear energy, has developed national satellite systems (ARSAT, SAOCOM), and has built a strong bioeconomy with notable achievements in agricultural biotechnology and vaccine production. Emerging AI ecosystems, although still small, reveal growing domestic expertise and an intention to develop digital tools tailored to national needs.

Active public policies reinforce autonomy in defense, health, agriculture, energy, education, and cybersecurity. These include local production of military systems and drones, national vaccine manufacturing, precision agriculture technologies, renewable-energy capacity development, digital inclusion programs, and a National Cybersecurity Strategy focused on building domestic capabilities.

Looking ahead, Argentina identifies a set of strategic technologies essential for future autonomy: artificial intelligence, big data, quantum computing, biotechnology, satellite and space systems, nanotechnology, robotics, additive manufacturing, and Industry 4.0 technologies. Developing local capacities in these fields is considered crucial to reduce external

dependency, strengthen sovereignty, and positioning the country competitively in the global knowledge economy.[42] [43] [44] [45] [46] [47] [48] [49]		
Defining Technological Sovereignty		
How is technological sovereignty defined in your jurisdiction? What are the most important factors considered? Examples of Factors: ● Political ● Social ● Dependency perspective ● IT Infrastructure ● Legislative perspective (various levels)	There is no legal definition. Technological sovereignty may be defined as the sovereign prerogative of a State to determine, autonomously and without external interference, the course of its economic, scientific, and technological development.	
Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?	No	**Explanation:** Argentina has not published a national cloud sovereignty policy. However, it has taken steps in this direction through different initiatives, such as: ● SIGEN Resolution No. 48/2005: Sets internal control standards for outsourcing IT services, including formal contracts, SLAs, and data ownership clauses. ● ONTI's official report (2021), which introduced the Cloud First policy, promoting the use of hybrid clouds and prioritizing local infrastructure for cloud services in the federal public sector, strengthening technological autonomy and data protection. This policy states that

[42] https://www.boletinoficial.gob.ar/detalleAviso/primera/333751/20251031
[43] https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf
[44] https://www.argentina.gob.ar/noticias/cientificos-del-centro-atomico-bariloche-buscan-crear-un-procesador-cuantico-con-circuitos
[45] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1992-D-2025.pdf
[46] https://www.state.gov/93-209/#:~:text=,and%20entered%20into%20force
[47] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1992-D-2025.pdf
[48] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-580-2011-185055
[49] https://www.boletinoficial.gob.ar/detalleAviso/primera/176168/20171215

		each agency is responsible for selecting its own cloud, migration, and data location, and that cloud providers must be qualified. ● Plan Conectar (2020-2023), which created the National Public Cloud (ARSAT) and expanded cloud services for public and private entities.
AI and Technology Sovereignty policy		
Has your jurisdiction published a national technology sovereignty policy?	No. But Strategic Guidelines in Innovation, Science, and Technology (2025–2027) was recently approved.	**Explanation**: As a national strategy for the development of the Science, Technology, and Innovation (STI) sector, the National Science, Technology and Innovation Plan 2030 is oriented toward the growth and diversification of institutional, organizational, and strategic management capacities, as well as their integration into productive development activities. These objectives entail the strengthening of scientific and technological capacities (human resources, equipment, and infrastructure) and their orientation toward addressing solutions identified as strategic for the country. The plan seeks to provide responses to productive demands and to promote public-private partnerships, technology transfer, and corporate investment in research, development, and innovation.[50]
Does your jurisdiction have a published national AI strategy/policy?	Yes. Argentine National Artificial Intelligence Plan	**Explanation**: The National Artificial Intelligence Plan aims to design and implement public policies that foster sustainable growth and equal opportunities in Argentina through the ethical and inclusive use of AI technologies. Its overarching goal is to position Argentina as a regional leader in AI development, promoting innovation across scientific, socioeconomic, political, and industrial spheres. Main objectives:

[50] https://www.boletinoficial.gob.ar/detalleAviso/primera/333751/20251031

		• Economic Growth and Adoption • Inclusive and Sustainable AI • Risk Mitigation • Talent and Research Development • Federal and Institutional Cooperation.[51]
Does your jurisdiction have a published AI compute or cloud strategy/policy?	No	**Explanation**: There is no AI compute or cloud strategy/policy, rather than the Argentine National Artificial Intelligence Plan.
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks related to technological sovereignty?	Digital sovereignty is a topic of current discussions in Argentina.	**Explanation**: In 2022 the national government invested over 199,277 USD to reduce the digital divide across the entire country. In this context, former Chief of Cabinet Juan Manzur stated that one of the former Government's goals was to achieve digital sovereignty.[52] In October 2023, the "First Regional Conference on Artificial Intelligence and Digital Sovereignty" was held in Buenos Aires, co-organized by the Secretariat of Public Innovation, the University of San Martín, and other institutions.[53] In 2025 the "Localization of Infrastructure and Data Storage in Servers Located within National Territory" legislative bill was proposed. This bill establishes restrictions on large-scale data transfers abroad, allowing them only for backup purposes in countries maintaining diplomatic relations with Argentina and preferably under reciprocal data protection standards, thus avoiding transfers to opaque or potentially hostile jurisdictions. Companies providing services in Argentina may carry out international data transfers only under specific conditions, ensuring the protection of digital

[51] https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf

[52] https://www.argentina.gob.ar/noticias/el-gobierno-nacional-invierte-mas-de-289-millones-de-pesos-para-reducir-la-brecha-digital

[53] https://www.argentina.gob.ar/noticias/conferencia-regional-inteligencia-artificial-y-soberania-digital

		sovereignty and control over Argentine citizens' information.[54]
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	Yes. ● Prometea (Public Sector) ● DoctIA (Private Sector) ● Indash (Private Sector)	**Explanation:** **Prometea**: The first predictive artificial intelligence system developed to serve the Judiciary. The AI system searches for the case title on the website of the Superior Court of Justice of the City of Buenos Aires, associates it with another number (linked to the main proceedings), and then accesses the Judicial Branch of the Autonomous City of Buenos Aires (Juscaba) website. It retrieves and reads first- and second-instance rulings, analyzes more than 1,400 legal opinions (issued during 2016 and 2017), and finally issues a prediction.[55] **DoctIA**: DoctIA is an AI-based application designed to accelerate and simplify the search for legal precedents. Its operation is very straightforward. The user only needs to paste a legal statement, and the system automatically finds related case law.[56] **Indash**: Indash is a collaborative platform that brings together the needs of influencers, content creators, and corporate marketing, positioning itself as the new model of co-creation in the world of social media.[57]
Does your jurisdiction have national AI research centres of excellence?	Yes. (1) INARIA (Argentine Institute of Artificial Intelligence)	**Links to AI research centres of excellence:** (1) https://www.inaria.ar/ (2) https://www.ialab.com.ar/ (3) CIAI

[54] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1992-D-2025.pdf

[55] https://www.pensamientopenal.com.ar/doctrina/47747-primera-inteligencia-artificial-predictiva-al-servicio-justicia-prometea

[56] https://www.utdt.edu/ver_nota_prensa.php?id_nota_prensa=21724&id_item_menu=6

[57] https://www.forbesargentina.com/innovacion/estos-argentinos-crearon-indash-ia-marketing-digital-junto-reconocidos-founders-mural-pedidosya-darwinai-n81172

	(2) IALAB (Innovation and Artificial Intelligence Laboratory, Faculty of Law, University of Buenos Aires) (3) CIAI (Interdisciplinary Artificial Intelligence Center)	
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes. Proyect QUANTEC	**Explanation**: The National Atomic Energy Commission (CNEA) is working on the development of a small-scale quantum processor using superconducting circuits, as well as on other initiatives aimed at ensuring that this emerging technology becomes part of everyday life.[58]
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech stack, funding and adoption:	**Please rate each component on a five point scale and circle the best option** (1 = non-existent; 2 = nascent; 3 = existing but insufficient; 4 = solidly in place; 5 = world leading): **1. AI compute (GPU-equipped) data centres** 1 **2** 3 4 5 **2. Domestically developed AI foundational models** 1 2 **3** 4 5 **3. Existence of large high-value databases in high-value sectors of economic activity** 1 **2** 3 4 5 **4. Availability of funding/financing for commercialization of innovation** 1 2 **3** 4 5 **5. Rates of AI adoption by organizations** 1 **2** 3 4 5 **6. Domestic quantum computing research, development and commercialization** 1 **2** 3 4 5	
Data Ownership/Exclusive Data Rights		

58 https://www.argentina.gob.ar/noticias/cientificos-del-centro-atomico-bariloche-buscan-crear-un-procesador-cuantico-con-circuitos

Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	No. But Confidentiality Law (Trade Secret) may apply to the protection of databases.	**Explanation**: In Argentina, there is no specific (or sui generis) right for the protection of databases. However, information on databases can be protected as a trade or industrial secret, only if it constitutes confidential information that grants a competitive advantage, is not generally known, has commercial value, and that reasonable measures have been taken to maintain its secrecy.[59]
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?	No	**Explanation**: No legal or administrative framework has yet been established in Argentina specifically regulating TDM activities. Argentina is often referred as an example of a country with a restrictive interpretation of copyright limitations and exceptions, which in practice "makes research through TDM almost impossible". Therefore, researchers or innovators wishing to extract data from copyrighted works must currently obtain express authorization from the rights holders or limit their activity to information not protected by copyright.[60] (Source) Argentina has implemented promotion regimes that, while not specifically aimed at TDM, benefit technology-based activities in which data mining is often included. The main instrument is the Knowledge Economy Regime under Law No. 27,506, which grants certain tax incentives to Argentine companies engaged in technology- and innovation-intensive sectors[61]
Does your jurisdiction have (1) an open, principle-based notion of "fair use" or (2) a closed, listed exceptions-based	Argentina has neither, just closed, listed exceptions. Intellectual Property Law No. 11.723[62]	**Explanation**: The Copyright Law provides for certain limited exceptions and limitations for the use of protected works, such as the use of works for educational purposes, quotations

[59] https://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm
[60] Link doesn't work
[61] https://www.argentina.gob.ar/normativa/nacional/ley-27506-324101
[62] https://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

notion of “fair dealing”? Do those rules favor national players?		under specific conditions, and the reproduction of news items of general interest. However, the law does not recognize a general fair use doctrine comparable to that of U.S. law, nor has such a principle been acknowledged in Argentine case law.[63]
Have courts in your jurisdiction issued decisions on the application of “fair dealing” or “fair use” in relation to the use of unlicensed data to train AI models (i.e. via screen scraping)?	No	**Explanation**: Argentine courts have not issued any decisions on the specific application of "fair use" or "fair dealing" for using unlicensed data to train AI models.
Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?	No	**Explanation**: In Argentina, beyond the general intellectual property and personal data protection frameworks, there are no special exclusivity rights provisions that establish “data ownership” in a strict proprietary sense. Personal data is protected under personality rights and Law No. 25,326 on Personal Data Protection, but not as commercial property of either the individual or the entity that collects them.
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: a) in the public sector? b) in the private sector?	a) No localization provisions b) No	**Explanation:** a) Even though there is no data localization obligation, in 2025, a bill is under parliamentary discussion that reintroduces the idea of mandatory data localization: it seeks to require that “all companies providing services in Argentina” store Argentine citizens’ personal data and strategic/sensitive information exclusively on servers physically located within the country. The bill defines “strategic sensitive information” (data essential for key sectors such as energy, health, and defense) and

[63] https://www.argentina.gob.ar/justicia/derechofacil/leysimple/propiedad-intelectual

		mandates its primary processing within Argentine territory.[64] b) There is no general rule requiring the domestic localization of all data. Private companies may, in principle, use data centers or cloud services located outside the country, if they comply with the Personal Data Protection Law No. 25,326 regarding international data transfers.
What are special classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?	Although they do not explicitly mandate that data "must be hosted within the country," in practice, public sector information security policies tend to keep within national territory those datasets whose disclosure could affect national security or the public interest.	**Explanation:** Law No. 25,326 defines sensitive data as ethnic origin, political opinions, religious beliefs, health, sexual life, biometric data and generally prohibits their processing, except under specific exceptions. However, the law does not mandate for this information to be only hosted within Argentina[65] For reasons of defense, security, or intelligence, certain government information is declared classified, secret, or restricted. National Intelligence Law No. 25,520 and its amendments prohibit intelligence agencies from collecting data on individuals based on their race, religion, political opinions, among others, and establish that intelligence information must be handled under security classification. Likewise, agents are bound by confidentiality obligations.[66]
What are the most notable cross-border data transfer restrictions in your jurisdiction?	Law 25,326 and its Regulatory Decree No. 1558/2001	**Explanation:** Article 12 of Law No. 25,326 prohibits the transfer of personal data to countries or international organizations that do not ensure adequate levels of protection, as determined by Argentine regulations. Through Resolution DNPDP 60-E/2016 and Resolution AAIP 34/2019, Argentina recognized as "countries with an adequate level of protection" all Member States of the European Union and the European

[64] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1992-D-2025.pdf
[65] https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[66] https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm

		Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faeroe Islands, Canada (only applicable to their private sector), New Zealand, Andorra, Uruguay, Israel (only for data treated by automated means), the United Kingdom of Great Britain and Northern Ireland.[67] If the destination country is not on the adequacy list (for example, the U.S. or Brazil), the transfer is only lawful if it falls under one of the special conditions set forth in Article 12(2) or if: (i) consent of the data subject is obtained; or approved contractual safeguards (such as standard contractual clauses or binding corporate rules) are implemented.[68]
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?	Resolution 198/2023: Standard Contractual Clauses	**Explanation:** The most recent notable regulatory decision was the approval of the Standard Contractual Clauses for International Data Transfers included in the "Guide for the Implementation of Standard Contractual Clauses for the International Transfer of Personal Data" of the Ibero-American Data Protection Network in 2023.[69]
Information Security Laws for Critical Infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Yes Resolution No. 580/2011 Resolution No. 44/2023	**Explanation**: Resolution No. 580/2011 establishes the National Program for Critical Information Infrastructure and Cybersecurity, with the purpose of promoting the creation and adoption of a specific regulatory framework aimed at identifying and protecting the strategic and critical infrastructures of the National Public Sector, interjurisdictional bodies, and civil and private sector organizations that may require it, as well as fostering collaboration among these sectors to develop appropriate strategies and structures for coordinated action toward the implementation of relevant technologies, among other measures.[70]

[67] https://www.argentina.gob.ar/sites/default/files/disp_e2016_60.pdf
[68] https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[69] https://www.boletinoficial.gob.ar/detalleAviso/primera/296189/20231018
[70] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-580-2011-185055

		Resolution No. 44/2023 – Objective No. 2: Protection of National Critical Infrastructures - Promote the development of strategies, policies, and action measures for the protection, operation, and communication of national critical infrastructures. To this end, it is necessary to: • Promote the definition and identification of the country's critical infrastructures related to information, operation, and communication. • Encourage public–private coordination for the protection of critical infrastructures, within the framework of each organization's respective responsibilities. • Strengthen cooperation in the exchange of information regarding cybersecurity vulnerabilities and threats. • Promote coordinated efforts within industrial data networks with the aim of strengthening and safeguarding critical and productive services. • Encourage greater investment by organizations in resources aimed at protecting their infrastructures.[71]
In your jurisdiction, can directors and officers be held accountable for not diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?	Yes Argentine Companies Law	**Explanation**: Under Argentine corporate law, directors and officers can be held liable if they fail to properly oversee risks associated with supplier concentration or the lack of diversification of critical digital infrastructure. Although there is no statute that specifically mandates technological or vendor diversification, these matters are governed by the general fiduciary duties established in the Argentine Companies Law (Ley General de Sociedades, "LGS"). Under Articles 59 and 274 LGS, directors must act with the diligence of a "good businessman" and are jointly and severally liable for damages arising from negligence, omission, or insufficient oversight. This includes a duty to identify core operational risks, monitor the stability and resilience of critical suppliers, and adopt reasonable

[71] https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

		mitigation measures where supplier-side concentration creates foreseeable operational or cybersecurity vulnerabilities. Reliance on a single provider for mission-critical digital infrastructure is considered a foreseeable and objectively assessable risk. If the board fails to evaluate alternatives, conduct and document risk assessments, obtain expert advice, or implement contingency planning, such inaction may amount to a breach of the duty of care or a failure-to-monitor scenario. While the business judgment rule protects informed and well-documented decisions, it does not shield inaction. Therefore, when supplier-concentration risks are foreseeable and remain unassessed or unmanaged, directors may face liability toward the company, its shareholders, and, depending on the industry involved, regulators. In short, while Argentina does not impose a stand-alone statutory obligation to diversify digital infrastructure, the general framework of fiduciary duties fully applies, and directors may be held accountable where concentration risks are evident and left unaddressed.
Lawful Access (Legal Access to Data without Consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?	Yes Law No 25,326 Law No.25.520	**Explanation**: Personal Data Protection Law No. 25,326 provides that consent from the data subject is not required, among others, when *"they are collected for the performance of functions inherent to the powers of the State or pursuant to a legal obligation"*. Article 18 of the National Intelligence Law provides that, when, in the course of intelligence or counterintelligence activities, it becomes necessary to intercept or capture private communications of any kind, the Intelligence Secretariat must request the corresponding judicial authorization. Such authorization must be made in writing and duly substantiated, precisely indicating the telephone numbers, electronic addresses, or any other means

		of communication whose content is intended to be intercepted or captured.[72]
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a "collect all" regime) under such lawful access regime?	No	**Explanation**: There are no explicit authorization in these provisions; the scope of permitted actions must be specified within the relevant legal instrument.
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?	No, only limited exceptions.	**Explanation** Law No. 25,326 provides that the party bound by confidentiality may be released from the duty of secrecy by a court order and when there are well-founded reasons relating to public security, national defense, or public health.[73] Article 216 of the Federal Criminal Procedure Code regulates apprehension without a judicial warrant. No person may be apprehended without a judicial warrant, except in the following cases: a. If the person is caught in the act of committing a crime (in flagrante delicto); b. If the person has escaped from a penal institution or any other place of detention. In cases of flagrante delicto, any person may carry out the apprehension in order to prevent the crime from producing further consequences. The apprehended person shall be immediately handed over to the nearest authority. The authority that has apprehended a person must immediately notify the judge and the representative of the Public Prosecutor's Office.[74]

[72] https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm

[73] https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm#:~:text=que%20permitan%20hacerlo.-,2.,datos%20de%20que%20se%20trate.

[74] https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/319681/norma.htm

Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Yes 1) Budapest Convention on Cybercrime 2) MLAT Argentina-USA 3) Convention 108+ (not yet in force)	**Explanation**: 1) Argentina is a party to the Budapest Convention, which sets standards for international cooperation in investigating cybercrime, including lawful access to data across borders.[75] 2) Argentina has signed a Mutual Legal Assistance Treaty (MLAT) in criminal matters with the United States since 1990, in force since 1993. This treaty establishes the procedure by which U.S. judicial authorities may request evidence (including data) in Argentina and vice versa, through Central Authorities.[76] 3) Argentina acceded to Convention 108 in 2019 and ratified its modernized Protocol, known as Convention 108+, in 2022. In terms of lawful access to data it reinforces that international transfers of personal data must safeguard individual rights (in line with Argentina's Law No. 25,326) and promotes cooperation among data protection agencies.[77]
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation? What is their most notable impact on promoting technological autonomy?	Competition Law (No. 27,442) Law No. 27,506 (amended by Law No. 27,570)	**Explanation**: Competition Law expressly prohibits anti-competitive practices that hinder technological progress, such as agreements to limit research and development (R&D) or to control innovation-related investments (art 3.e). By preventing dominant companies from blocking the entry of new players or agreeing on restrictions in technical developments, the regulation creates a dynamic competitive environment that encourages all companies to innovate

[75] https://www.boletinoficial.gob.ar/detalleAviso/primera/176168/20171215

[76] https://www.mpf.gob.ar/cooperacion-ai/files/2016/09/Ley-24034-Tratado-de-Asistencia-Jur%C3%ADdica-Mutua-con-Estados-Unidos.pdf

[77] https://www.argentina.gob.ar/noticias/se-convirtio-en-ley-la-aprobacion-del-convenio-108

		continuously. It has been used by competition authorities to prevent economic concentrations that could harm local technological development.[78] The Knowledge Economy Regime, aimed at fostering the development of activities that rely heavily on technology and skilled human capital, promoting the creation of quality employment and added value within the country. This law grants tax benefits to Argentine companies to encourage sectors like software, biotechnology, and professional services.[79]
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?	Yes	Explanation: There are several cases in which the Argentine Antitrust Authority (*Autoridad Nacional de la Competencia* or "ANC"; formerly the *Comisión Nacional de Defensa de la Competencia* or "CNDC") applied Law 27,442 to foster competition and ensure autonomy and innovation in technological markets, namely: **Opening Up the Digital Payments Ecosystem:** In 2016, the Argentine Antitrust Authority initiated an ex officio investigation against Prisma Medios de Pago and its bank shareholders for alleged anticompetitive practices in the electronic payments market. The case focused on Prisma's exclusive role as the sole acquirer and processor of Visa transactions in Argentina, raising concerns about market foreclosure, restricted access to payment infrastructure, and barriers to entry for fintech competitors. In 2017, the Argentine Antitrust Authority imposed the divestiture of Prisma, which dismantled the vertical integration between banks and the acquiring business. This case reshaped the digital payments ecosystem in Argentina and laid the foundations for fintech players to enter the market with new technological

[78] https://www.boletinoficial.gob.ar/detalleAviso/primera/183602/20180515
[79] https://www.argentina.gob.ar/normativa/nacional/ley-27506-324101/actualizacion

		solutions, fostering innovation and expanding competitive alternatives.[80] **Merger Review of Two Major Entertainment Companies:** The Argentine Antitrust Authority applied Law 27,442 to address concerns that the consolidation of two major foreign media and technology players could undermine local technological development and reinforce structural dependence on external providers. The regulatory interventions, focused on market concentration in audiovisual distribution, control over content pipelines, and potential foreclosure of domestic competitors, demonstrate how competition law can be used to safeguard space for local innovation and prevent excessive dominance by global platforms.[81] **Merger Review of Two Major Entertainment Companies:** The Argentine Antitrust Authority competition authorities applied Law 27,442 to address concerns that the consolidation of two major foreign media and technology companies could undermine local technological development and reinforce structural dependence on external providers. The regulatory interventions, focused on market concentration in audiovisual distribution, control over content pipelines, and potential foreclosure of domestic competitors, demonstrate how competition law can be used to safeguard space for local innovation and prevent excessive dominance by global platforms.[82] **Banks vs. the Leading Fintech Platform:** On 2024 a complaint was filed by major Argentine banks before the Argentine

80 https://www.argentina.gob.ar/noticias/con-la-venta-de-prisma-se-abre-una-etapa-de-mas-competencia-y-nuevas-inversiones

81 https://www.argentina.gob.ar/noticias/fusion-disney-fox-la-cndc-dictamino-la-desinversion-y-puso-condiciones-para-garantizar-la

82 https://www.argentina.gob.ar/noticias/fusion-disney-fox-la-cndc-dictamino-la-desinversion-y-puso-condiciones-para-garantizar-la

		Antitrust Authority National Commission for the Defense of Competition (CNDC) against the principal e-commerce operator in the region for alleged anticompetitive practices in the digital payments ecosystem. Although the investigation is still ongoing, the case shows how competition law is increasingly applied to high-impact technology markets where a single dominant platform controls critical digital infrastructure, user data flows, and transaction channels. By scrutinizing the market power of a leading fintech actor, the Argentine Antitrust Authority authorities are is indirectly addressing structural risks that affect technological autonomy – such as excessive dependence on one provider, barriers to entry for local competitors, and reduced diversification of digital infrastructure.[83] **<u>Telecom Industry Consolidation</u>:** Recently, the Argentine Antitrust Authority Argentine National Competition Commission (CNDC) issued a *Statement of Objection* regarding the leading telecom operator Argentina's proposed acquisition of Telefónica Móviles Argentina. The authority found that the transaction could restrict competition across several telecom markets. It would reduce the number of national mobile operators from three to two, create excessive spectrum concentration beyond ENACOM limits, and generate high or dominant market shares in fixed internet and fixed telephony in more than 180 localities. The deal would also make the leading telecom operator the only operator capable of offering nationwide quad-play services and give it a dominant position in corporate telecom services. Due to these risks to competition and the general economic interest, the Argentine Antitrust Authority CNDC called a special hearing to explore potential remedies.[84]

[83] https://www.infobae.com/economia/2024/05/06/los-bancos-denunciaron-a-mercado-libre-ante-el-gobierno-por-practicas-anticompetitivas/

[84] https://www.argentina.gob.ar/noticias/informe-de-objecion-operacion-telecom-telefonica

Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes") ?	Yes 1) Argentina - USA MLAT	**Explanation**: 1) The MLAT requires compliance with local judicial procedures and safeguards in order to obtain evidence (including data). It enables and requires cross-border access to, and transfer of evidence and data held by the Argentine State, allows for searches and seizures ordered by a foreign State, and establishes flows of non-public governmental information. It also provides safeguards, such as: ● the possibility of denying assistance on grounds of national security, ● the authority to impose conditions or postpone deliveries, ● and limits on the use of the information.[85]
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	No. Argentina currently does not have "buy local" federal procurement rules specifically applicable to advanced technology equipment or services.	**Explanation**: Historically, Law 27.437 (Compre Argentino y Desarrollo de Proveedores) established a general national preference regime that applied across all sectors, including technology. However, Law 27.437 was expressly repealed by Decree 70/2023, a broad deregulatory emergency decree issued in December 2023, which eliminated the national preference system for public procurement.
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose	Yes 1) Knowledge-Economy Promotional Regime (Law No. 27,570)	**Explanation**: 1) Knowledge Economy Promotional Regime: Argentine tech companies and companies engaged in the performance of activities associated with the knowledge-based

[85] https://www.state.gov/93-209/#:~:text=.and%20entered%20into%20force

restrictions on origin of the funds and the manner in which they are invested?	2) Biotech and Nanotech Promotional Regime (Law 26,270) 3) Promotion and Development of Technological Innovation (Law No. 23,877)	economy[86] can apply to this regime, which is a tax incentive program created under Law No 27,570 (as amended). The regime, in force until year 2029, aims to promote new technologies, generate added value, encourage quality employment, facilitate the development of MSMEs, and increase exports of companies engaged in knowledge-based services. Beneficiaries to this regime enjoy a significant reduction of their corporate income tax rate (60% for micro and small enterprises, 40% for medium-sized enterprises, and 20% for large enterprises), and a tax credit bonds of up to 70% of the paid social security contributions to cancel other federal taxes, among other benefits.[87] 2) Biotech and Nanotech Promotional Regime: The Biotech and Nanotech Promotional Regime, created under Law 26,270 (as amended) and in force until 2034, is directed to Argentine companies working on: (a) R&D projects based on the application of modern biotechnology/nanotechnology or (b) projects that apply modern biotechnology/nanotechnology for manufacturing goods, performing services or improving existing procedures or products. The regime provides certain tax benefits for the development of the project such as: (a) VAT reimbursements; (b) accelerated depreciation of capital goods affected to the promoted project, and (c) the granting of tax credit bonds which can be used for

[86] The KE Regime promotes many activities, among others: software, computer and digital services; audiovisual production and post-production; biotechnology, neurotechnology and genetic engineering; geological and prospecting services and others related with electronic and communications; professional services as long as they are exported; nanotechnology and nanoscience; aerospace and satellite industry; nuclear industrial engineering; artificial intelligence, robotic and industrial internet, the internet of things, augmented and virtual reality.

[87] https://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/343521/norma.htm

		paying advances and/ or balances of other federal taxes, among others.[88] 3) Law No. 23,877 proposes to improve productive and commercial activity through the promotion and encouragement of research and development, technology transfer, technical assistance, and all other innovative actions that contribute to achieving greater well-being for the people and the nation's progress, while socially elevating the role of scientists, technologists, and innovative entrepreneurs. Among other benefits, Argentine companies investing in R&D and technological innovation may be eligible for a tax credit bond equivalent to a percentage of the expenses incurred in this field.[89] In general, all these regimes do not impose restriction on origin of the funds or the manner in which they are invested. However, the Knowledge Economy Promotional Regime requires certain minimal annual investments in R&D, training of the personnel, etc. as established in the law.
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?	Yes Data Protection Law by European Standards	**Explanation**: Argentine Data Protection Law No. 25,326 (DPL) is inspired in The European Union regulation on data privacy matters. Argentina became the first Latin American country with a data protection law deemed "adequate" by the EU, which ensured data flows from Europe but also meant incorporating foreign principles into local legislation. There are currently several bills proposals to modify the current DPL. Three initiatives aim to modernize Argentina's data

[88] https://www.argentina.gob.ar/normativa/nacional/ley-26270-2007-130522
[89] https://www.argentina.gob.ar/normativa/nacional/ley-23877-277/actualizacion

		protection framework, aligning it with international standards. They incorporate innovative concepts such as anonymization, biometric data, automated decision-making, and profiling.
Ongoing / Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?	Yes Bill 1992-D-2025	Explanation: If passed, the bill 1992-D-2025 would require all companies providing services in Argentina -whether domestic or foreign- to store Argentine citizens' personal data and strategic or sensitive information exclusively on servers located within national territory. It mandates that such data be processed in line with Argentina's data protection principles, ensuring security, integrity, and confidentiality. The State must guarantee that primary storage and processing occur domestically, allowing secondary backups abroad only if strict protection standards are met. Overall, the proposal seeks to strengthen digital sovereignty, keeping critical and personal data under Argentine jurisdiction and safeguarded from foreign interference. The bill would strengthen Argentina's technological autonomy by ensuring that critical and personal data remain under exclusive national jurisdiction. By requiring local storage and domestic processing, it limits the extraterritorial reach of foreign laws -such as the U.S. Cloud Act- and reduces dependence on foreign infrastructure and cloud providers. This, in turn, incentivizes investment in local data centers, enhances national cybersecurity, and preserves Argentina's ability to regulate data according to its own legal and ethical standards. Overall, the proposal reinforces digital sovereignty, mitigates foreign interference risks, and empowers Argentina to develop its own innovation ecosystem built on domestically controlled data.[90]

[90] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1992-D-2025.pdf

Canada

Charles Morgan, McCarthy Tétrault LLP, Montreal
Francis Langlois, McCarthy Tétrault LLP, Montreal
Esther Gao, McCarthy Tétrault LLP, Montreal

Executive summary

Few countries in the world are as economically integrated as the United States and Canada. In 2024, Canada was the largest importer of US goods in the world and the US's third largest source of imported goods (after China and Mexico). Nevertheless, in the context of the current US government's dramatic recent shifts in trade and military policy, Canada has had to radically reassess this relationship and its implications for Canada's resilience and autonomy. Canadian Prime Minister Mark Carney stated in March 2025 that Canada's old relationship with the United States, "based on deepening integration of our economies and tight security and military cooperation, is over".[91]

Canada's new economic reality has brought with it a heightened awareness of its fundamentally unhealthy reliance on a single economic partner and a new resolve to increase its economic, technological and military autonomy. In particular, Canada has begun to focus increasingly on the removal of internal trade barriers (as between provinces) and to increase trade with partners in both Asia and Europe, in the hope that increased "East-West" trade will offset losses in "North-South" trade with the aim of doubling non-US exports over the next decade.[92]

In this context, one of the very first acts of the newly elected Carney government was to adopt "An Act to enact the Free Trade and Labour Mobility in Canada Act and the Building Canada Act".[93] Part 1 of the act establishes a statutory framework to remove federal barriers to the interprovincial trade of goods and services and to improve labour mobility within Canada. Part 2, referred to as the "Building Canada Act" is designed to "enhance Canada's prosperity, national security, economic security, national defence and national autonomy by ensuring that projects that are in the national interest are advanced through an accelerated regulatory process. Canada has also aggressively pursued new free trade deals, including with Indonesia.[94]

In this context, technological sovereignty has become a matter of particularly focused concern in Canada. Canada is widely acknowledged to be a global leader in fundamental AI research, with multiple world-renowned universities and research centers, supported by the Pan-Canadian Artificial Intelligence Strategy[95], the world's first national strategy dedicated to AI. Although those capacities have helped Canada play a key role in the research and development of AI technologies, Canada has so far struggled in moving research into products and commercialization, with certain notable exceptions like foundational models provider Cohere.

Canada is also generally dependent on foreign hyperscalers for cloud hosting and AI compute capacity, which has led to renewed concerns related to foreign companies and foreign governments having access to Canadian data. Revisiting themes and concerns that had initially first been raised (and largely resolved[96]) following the adoption of the USA PATRIOT Act in

[91] Carney says he'll speak to Trump soon, promises to fight back on auto tariffs (CBC).
[92] https://financialpost.com/news/carney-doubling-canada-non-us-exports
[93] One Canadian Economy Act - Parliament of Canada
[94] Canada-Indonesia Comprehensive Economic Partnership Agreement (CEPA)
[95] Pan-Canadian Artificial Intelligence Strategy
[96] Guidelines for processing personal data across borders - Office of the Privacy Commissioner of Canada

2001, the Canadian government and many private sector enterprises are currently re-examining the implications and perceived risks associated with the U.S. CLOUD Act of 2018.

In this context, Canada has appointed its first federal Minister of Artificial Intelligence and Digital Innovation, Evan Solomon, with a mandate to boost AI adoption, increase trust in AI, and build sovereign AI architecture. In October 2025, the Canadian Federal government published a framework to promote digital sovereignty, defined as "the ability of the [Government of Canada] to exercise autonomy over its digital infrastructure, data and intellectual property".[97] Amplifying an international trend to promoting "thicker borders" as regards trans-border data transfers of sensitive data, the framework acknowledged that storing data in Canada or with Canadian service providers does not in itself guarantee data will be outside the jurisdiction of foreign courts and stated that the Government of Canada ("GC") "can fully maintain legal control only when it delivers services itself or works with providers that operate entirely under Canadian jurisdiction".[98]

Recent federal budgets have included investments underscoring commitments to strengthen Canada's technological infrastructures, including the "Canadian Sovereign AI Compute Strategy" (2024) with $2 billion earmarked until 2030 to develop domestic high-performance computing for AI. Likewise, Canada's National Quantum Strategy (2023) dedicates $360 million to quantum research, talent, and commercialization, aiming to solidify Canada's leadership in quantum technologies. Those investments remain however modest when compared against investments by leading foreign private tech firms.

Acknowledging that an overly prescriptive "fair dealing" regime under Canada's Copyright Act may discourage homegrown efforts to train AI models in Canada, the Government of Canada conducted a Consultation on Copyright in the Age of Generative Artificial Intelligence between October 12, 2023, and January 15, 2024, to better understand the effects of generative artificial intelligence (AI) on copyright and the marketplace. The results of the consultation have so far been inconclusive[99] and no amendments to the Copyright Act have yet been adopted.

Although AI, advanced computing, cloud and 5G networks are currently the main focus of Canadian technology autonomy policy and efforts, the Carney government has also looked to diversify its military spending to reduce over-reliance on the United States, ordering a review of Canada's plan to purchase a fleet of F-35 fighter jets under an existing deal with Lockheed Martin and the US government, while pursuing negotiations with Swedish defense company Saab and the Canadian aerospace company Bombardier to build the Saab Gripen fighter jet under license in Canada[100], while potentially turning to German and South Korean suppliers (instead of US suppliers) in relation to an anticipated purchase of new military submarines.

Astonishingly (for Canadians used to the comfort of living along the longest undefended border in the world), the Canadian department of national defence has recently has set in motion a

---

[97] Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada - Canada.ca

[98] With a call out to foreign lawful access regimes (such as the US CLOUD Act), the Digital Sovereignty Framework expressly noted that "The GC could find no documented cases of foreign governments seeking access to the data of Canadian enterprises held by suppliers." At the same time, it is noteworthy, that Canadian privacy commissioners recently flagged concerns regarding the transfer of personal information about Canadians by TikTok operator, ByteDance, to its parent company in Mainland China: PIPEDA Findings #2025-003: Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta - Office of the Privacy Commissioner of Canada

[99] Consultation on Copyright in the Age of Generative Artificial Intelligence: What we heard report

[100] Sweden's Saab offers to build entire GlobalEye military surveillance plane in Canada - The Globe and Mail

Whole of Society (WoS) effort (partly inspired by leading initiatives in Finland and focused primarily on perceived emerging threats from Russia and China) that would include increasing the size of our "Supplementary Reserve" from 4,384 personnel to 300,000 reserves, calling on public servants to volunteer for a one-week training course in how to handle firearms, drive trucks and fly drones as part of an overall mobilization plan.[101]		
Defining Technological Sovereignty		
How is technological sovereignty defined in your jurisdiction? What are the most important factors considered? Examples of Factors: ● Political ● Social ● Dependency perspective ● IT Infrastructure ● Legislative perspective (various levels)	**Definition of digital sovereignty by the Federal government:** For the Government of Canada (GoC), digital sovereignty is defined as the ability of the GC to exercise autonomy over its digital infrastructure, data and intellectual property. It is the capacity to operate effectively and make independent decisions about digital assets, regardless of where technologies are developed, hosted, or supported. The concept does not imply "isolation"[102].	
Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?	No. But, it published a GC Whitepaper, which applies to the public sector, on Data Sovereignty and Public Cloud in 2018[103]	The Government of Canada (GC) has a "cloud-first" strategy whereby cloud services are identified and evaluated as the principal delivery option when initiating information technology (IT) investments, initiatives, strategies and projects. The Treasury Board of Canada Secretariat (TBS), in consultation with key departments, has determined that a commercial public cloud can, under certain conditions, offer sufficient protections for data up to and including the "Protected B" level. The GC whitepaper notes that limiting residency to Canada introduces 2 new risks: 1. Limiting data storage to Canada may limit the market availablility of solutions. At the time of writing, at

[101] Top general plans sweeping expansion of reserves for disasters, military attacks - The Globe and Mail
[102] Government of Canada, *Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada* (October 2025), https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html.
[103] Government of Canada White Paper: Data Sovereignty and Public Cloud - Canada.ca was published in 2028

		least 5 of the largest cloud service providers (CSPs) have the ability to isolate data in Canada. 2. Limiting data storage to Canada may be viewed as being a barrier to trade.
AI and Technology Sovereignty Policy		
Has your jurisdiction published a national technology sovereignty policy?	No. But it published a Digital Sovereignty Framework[104] for the public sector.	The Federal government published in October 2025 a framework for digital sovereignty which identifies several challenges Canada faces to its digital sovereignty such as the challenges in maintaining control over government data, dependencies on global supply chains and retention of expertise. The Framework proposes to address digital sovereignty risks via procurement, supply and technological controls, including: - focusing on strengthening contractual clauses related to data access, disclosure, and business continuity to mitigate risks to confidentiality of data, availability of supply, and risk of deplatforming, including those heightened using AI and machine learning technologies. - strengthening guidance on the existing data residency and other policy requirements. - exploring means of improving supply chain visibility and assurance, including reviewing business continuity and disaster recovery planning to address potential service disruptions, loss of access, or deplatforming events. - exploring the use of vendor-neutral formats, GC-controlled environments, and strengthened encryption practices.

[104] Government of Canada, *Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada* (October 2025), https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html.

Does your jurisdiction have a published national AI strategy/policy?	Yes Pan-Canadian Artificial Intelligence Strategy and related initiatives (AI Safety Institute, Voluntary Code of Conduct, Advisory Council on AI).	The Pan-Canadian Artificial Intelligence Strategy focuses on: • AI research and talent • Commercialization and adoption of AI • AI policy, standards, and responsible use frameworks • Building AI capacity across sectors[105,106]
Does your jurisdiction have a published AI compute or cloud strategy/policy?	No	Although Canada does not have a published AI compute strategy/policy, the Government of Canada has announced its intention to develop a "Canadian Sovereign AI Compute Strategy" and has committed $2.4B in funding[107].
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks related to technological sovereignty?	Yes	Technological sovereignty has become a very lively topic in Canada, becoming a core theme at the recent ALL-IN conference in Montreal, the largest AI event in Canada.
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	Yes Cohere	Enterprise AI: Private, Secure, Customizable | Cohere[108]
Does your jurisdiction have national AI research centres of excellence?	Yes **Examples:**	Links to AI research centres of excellence: (1) Amii: https://fr.amii.ca/ (2) Mila: https://mila.quebec/en

[105] Government of Canada, *Pan-Canadian Artificial Intelligence Strategy* (October 2025), https://ised-isde.canada.ca/site/ai-strategy/en
[106] Government of Canada, *Canada partners with Cohere to accelerate world-leading artificial intelligence* (August 2025), https://www.canada.ca/en/innovation-science-economic-development/news/2025/08/canada-partners-with-cohere-to-accelerate-world-leading-artificial-intelligence.html
[107] ICTC, *Advancing Canada's National Sovereign AI Compute Capacity: An ICTC Policy Brief* (September 2025), https://ictc-ctic.ca/policy-briefs/advancing-canadas-national-sovereign-ai-compute-capacity
[108] https://cohere.com/

	(1) Amii (Alberta Machine Intelligence Institute) (2) Mila (Quebec Artificial Intelligence Institute) (3) Vector Institute for Artificial Intelligence (4) TELUS AI Factory	(3) Vector: https://vectorinstitute.ai/ (4) TELUS opens Canada's first fully Sovereign AI Factory [109]
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes (1) D-Wave (2) PINQ²	(1) D-Wave is a Canadian company and a global leader in quantum computing systems, software, and services. It is the world's first commercial supplier of quantum computers and the only company building both annealing and gate-model quantum computers[110]. (2) PINQ² offers hybrid quantum computing services and a Center of Excellence for quantum software development. Supported by partnerships with Hydro-Québec, Université de Sherbrooke, and IBM, this initiative accelerates quantum adoption and talent development[111].
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech stack, funding and adoption.	**Please rate each component on a five point scale and circle the best option** (1 = non-existent; 2 = nascent; 3 = existing but insufficient; 4 = solidly in place; 5 = world leading): 1. **AI compute (GPU equipped) data centres** 1 2 3 4 5 2. **Domestically developed AI foundational models** 1 2 3 4 5	

[109] Schmelzer, R., *Canada Joins The Global Push For Sovereign AI With TELUS AI Factory* (September 2025), Forbes, https://www.forbes.com/sites/ronschmelzer/2025/09/28/canada-joins-the-global-push-for-sovereign-ai-with-telus-ai-factory/

[110] D-Wave, *About D-Wave* (2025), https://www.dwavequantum.com/company/about-d-wave/

[111] IBM Newsroom, *The Platform for Digital and Quantum Innovation of Quebec (PINQ²) Proudly Announces the Historic Inauguration of an IBM Quantum System One Quantum Computer in Bromont* (September 2023), https://newsroom.ibm.com/2023-09-22-The-Platform-for-Digital-and-Quantum-Innovation-of-Quebec-PINQ-Proudly-Announces-the-Historic-Inauguration-of-an-IBM-Quantum-System-One-Quantum-Computer-in-Bromont

	3. Existence of large high-value databases in high-value sectors of economic activity 1 2 3 4 5 **4. Availability of funding/financing for commercialization of innovation** 1 2 3 4 5 **5. Rates of AI adoption** 1 2 3 4 5 **6. Domestic quantum computing research, development and commercialization** 1 2 3 4 5 **7. Domestic military defence industry** 1 2 3 4 5	
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	No	There is no separate (or sui generis) statutory protection for databases in Canada[112].
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?	No	Canada does not currently have a special statutory regime for TDM or a specific exception to promote research and commercialization of innovation in this area. The government is actively consulting on the issue, and legislative changes may be considered in the future, but no such regime exists as of 2025[113].
Does your jurisdiction have (1) an open, principle-based notion of "fair use" or (2) a closed, listed exceptions-based notion of "fair dealing"? Do those rules favor national players?	Canada has a "fair dealing" doctrine	In Canada, fair dealing is a closed, exception-based system. Only these listed purposes qualify[114]. Some argue that the current closed, exception-based definition of fair dealing in Canada makes unlicensed "screen scraping" for the purpose of model development more legally risky in Canada than in other

[112] ICLG, *Copyright Laws and Regulations (Canada)* (November 2025), https://iclg.com/practice-areas/copyright-laws-and-regulations/canada

[113] Government of Canada, *Consultation on Copyright in the Age of Generative Artificial Intelligence: What we heard report* (February 2025), https://ised-isde.canada.ca/site/strategic-policy-sector/en/marketplace-framework-policy/consultation-copyright-age-generative-artificial-intelligence-what-we-heard-report

[114] Simon Fraser University, *What is fair dealing and how does it relate to copyright?* (February 2024), https://www.lib.sfu.ca/help/academic-integrity/copyright/fair-dealing

		jurisdictions that have a principle-based fair use exception or a fit for purpose TDM exception.
Have courts in your jurisdiction issued decisions on the application of "fair dealing" or "fair use" in relation to the use of unlicensed data to train AI models (i.e. via screen scraping)	No	Canadian courts have not yet decided that fair dealing applies to the use of unlicensed data to train AI models. The outcome is uncertain and would depend on how the courts apply the established fair dealing framework to the facts of a specific case[115].
Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?	No	N/A
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: a) in the public sector? b) in the private sector?	**Examples:** Public sector: (1) Policy on Service and Digital (2) Directive on Service and Digital (3) *Personal Information International Disclosure Protection Act* (PIIDPA) of Nova Scotia Private sector:	(1) The Policy on Service and Digital establishes unified rules for how Government of Canada organizations manage services, data, IT, and cybersecurity[116]. (2) Articulates how Government of Canada organizations manage service delivery, information and data, information technology, and cyber security in the digital era[117]. (3) Requires that personal information held by Nova Scotia public bodies and their service providers be stored and accessed only in Canada, except in very limited and regulated circumstances[118]. (4) Section 17 of Law 25 applies to any "person carrying on an enterprise", which means it is aimed at private-sector

[115] The University of British Columbia, Peter A. Allard School of Law, *AI & Fair Dealing: Thomson Reuters v Ross Intelligence* (April 2024), https://iplaw.allard.ubc.ca/2025/04/17/ai-fair-dealing-thomson-reuters-v-ross-intelligence/#:~:text=Canada%2C%20as%20we%20all%20well%20know%2C%20has%20a,Canadian%20Ltd%20v%20Law%20Society%20of%20Upper%20Canada

[116] Government of Canada, *Policy on Service and Digital* (August 2025), https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603

[117] Government of Canada, *Directive on Service and Digital* (August 2025), https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601

[118] Nova Scotia Legislature, *Personal Information International Disclosure Protection Act,* https://nslegislature.ca/sites/default/files/legc/statutes/persinfo.htm

	(4) Quebec law 25	organizations that collect, hold, use, or communicate personal information in the course of their business activities[119].
What are special classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?	Protected and Classified levels of information	The GC has a classification system for protected Information (non-national interest; harm to individuals or organizations if compromised) that currently still permits for protected information up to "protected B" status to be store in the public cloud. Classified Information (national interest; harm to Canada's security or stability if compromised): ● Confidential – Injury to national interest. ● Secret – Serious injury to national interest. ● Top Secret – Exceptionally grave injury to national interest. *Requires high-security zones and facility clearances; generally cannot be stored outside Canada[120].*
What are the most notable cross-border data transfer restrictions in your jurisdiction?	(1) *Personal Information Protection and Electronic Documents Act* (Federal) (2) *Act Respecting the Protection of Personal Information in the Private Sector* (Quebec Privacy Act) Note: on the provincial level, BC and Alberta's privacy laws also	(1) If a Canadian organization transfers personal information to another Canadian or international organization, it remains responsible for ensuring that the information continues to receive a comparable level of protection[122]. (2) Before communicating personal information outside Quebec, organizations must conduct a privacy impact assessment (PIA)[123].

[119] Légis Québec, *Chapter P-39.1 - Act respecting the protection of personal information in the private sector*, https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1?langCont=en
[120] Government of Canada, *Levels of security* (December 2024), https://www.canada.ca/en/public-services-procurement/services/industrial-security/security-requirements-contracting/safeguarding-equipment-sites-assets-information/levels-security.html
[122] Government of Canada, *Personal Information Protection and Electronic Documents Act*, https://laws-lois.justice.gc.ca/eng/acts/P-8.6/
[123] Légis Québec, *Chapter P-39.1 - Act respecting the protection of personal information in the private sector*, https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1?langCont=en

	impose cross-border data transfer restrictions or applicable regulatory requirements.[121]	
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?	(1) *Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta* (2025) (2) *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (2019)	(1) The Offices found that TikTok's privacy policy referenced cross-border transfers, but that more up-front and detailed notice was required for meaningful consent. (2) The report confirms that Canadian privacy law (PIPEDA and BC PIPA) applies to cross-border data transfers, and organizations must ensure meaningful consent, transparency, and adequate safeguards when disclosing Canadians' personal information to third parties outside Canada. Facebook failed to meet these requirements, particularly in the context of the Cambridge Analytica scandal, where Canadian data was disclosed to foreign entities without proper consent or protection[124]. (3) This case shows that Canadian privacy law applies to Canadian organizations' handling of personal information, even if the data was collected in another country[125].

[121] Government of BC, *Freedom of Information and Protection of Privacy Act*, https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00, as amended by Bill 22, https://www.bclaws.gov.bc.ca/civix/document/id/bills/billscurrent/gov22-1_43rd1st

[124] Office of the Privacy Commissioner of Canada, *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (April 2019), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/

[125] Office of the Privacy Commissioner of Canada, *Joint investigation of AggregateIQ Data Services Ltd. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (November 2019), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-004/

	(3) *Joint investigation of AggregateIQ Data Services Ltd. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (2019)	
Information Security Laws for critical infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Critical Infrastructure information security bill currently before federal parliament	See discussion of Bill C-8 below
In your jurisdiction, can directors and officers be held accountable for not diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?	In theory, yes *Canada Business Corporations Act* (CBCA)	Under the CBCA, directors and officers have two principal fiduciary duties: a duty of care and a duty of loyalty. The duty of care imposed by CBCA requires that each director and officer of a corporation, in exercising their powers and discharging their duties, must exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances. The duty of care requires that directors and officers make sufficient inquiries to inform themselves and consider all material information available to them prior to acting. Managing risk is a core function of board oversight. Courts assess “reasonableness” by whether boards sought relevant information and exercised prudence in acting on that information in the best interests of the company.
Lawful Access (Legal access to data without consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by	**Examples:** (1) *Criminal Code* s. 487 (2.1) (2) PIPEDA s. 7(3)(c)	**Explanation:** (1) A person authorized to search a computer system under this section may use the system to search for data, reproduce the data as printouts or other readable formats, seize these outputs for examination or copying, and

telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?	(3) *Security of Canada Information Disclosure Act* (SCIDA) s. 3 Note that several other federal and provincial statutes (e.g., *Competition Act*) grant specific government agencies or departments the right to access personal information without consent in defined circumstances.[126]	use any copying equipment on site to make copies of the data. (2) Requires organizations to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records. Note that PIPEDA s. 7(3)(c) does not independently confer lawful authority to access data; it merely provides an exception to the consent requirement, which must be linked to another statutory provision granting the necessary legal authority. (3) Facilitates the disclosure of information between Government of Canada institutions in order to protect national security.
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a "collect all" regime) under such lawful access regime?	No	There does not appear to be any explicit authorization in these provisions; the scope of permitted actions must be specified within the relevant legal instrument. [127]
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?	No	Only in exceptional circumstances justifying urgency[128]
Has your jurisdiction entered in treaties or cooperation agreements	Yes	(1) Canada is a party to the Budapest Convention, which sets standards for international cooperation in investigating

[126] Government of Canada, *Competition Act* (R.S.C., 1985, c. C-34), https://laws-lois.justice.gc.ca/eng/acts/c-34/

[127] Office of the Privacy Commissioner of Canada, The *Personal Information Protection and Electronic Documents Act* (PIPEDA) (September 2025), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[128] Canadian Journal of Law and Technology, *The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information*, 2017 CanLIIDocs 4239, https://www.canlii.org/en/commentary/doc/2017CanLIIDocs4239#!fragment//BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoByCgSgBpltTCIBFRQ3AT0otokLC4EbDtyp8BQkAGU8pAELcASgFEAMioBqAQQByAYRW1SYAEbRS2ONWpA

that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Examples: (1) Budapest Convention on Cybercrime (2) Canada-U.S. Cloud Act Agreement (not yet in force)	cybercrime, including lawful access to data across borders.[129] (2) If in force, the Canada-U.S. CLOUD agreement would give U.S. law enforcement broad new powers to request personal data directly from Canadian digital service providers with U.S. connections, allowing them to access information in Canada without going through Canadian authorities. The new system would expose personal data stored in Canada directly to U.S. police surveillance, bypassing Canadian court oversight [130]
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation? What is their most notable impact on promoting technological autonomy?	*Competition Act* (R.S.C., 1985, c. C-34)	The *Competition Act* is the main law governing competition, merger review, and anti-competitive practices, with a focus on how changes may impact innovation and the tech sector.[131]
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?	No	No specific provisions have been used explicitly for such purpose in the competition law context. However, the Competition Bureau's approach is intended to foster Canadian innovation and competition.[132]

[129] Government of Canada, *Council of Europe Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, (October 2023), https://www.justice.gc.ca/eng/cj-jp/cyber/id-di/index.html#:~:text=Canada%20is%20Party%20to%20the%20Council%20of%20Europe,and%20the%20prosecution%20of%20cybercrimes%20and%20cyber-related%20crimes.

[130] Khoo, C. & Robertson, K. (February 2025), *Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under U.S. CLOUD Act*, https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/

[131] Freeman, A. (April 2024), *Does competition law and Canada's foreign investment review enable or hinder innovation?* https://nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2024/tech-and-merger-review

[132] Government of Canada, Council of Europe Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (October 2023), https://www.justice.gc.ca/eng/cj-jp/cyber/id-di/index.html#:~:text=Canada%20is%20Party%20to%20the%20Council%20of%20Europe,and%20the%20prosecution%20of%20cybercrimes%20and%20cyber-related%20crimes.

Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes") ?	Yes Examples: (1) Canada-United States-Mexico Agreement (CUSMA) (2) Canada-European Union Comprehensive Economic and Trade Agreement (CETA)	(1) The CUSMA agreement could place constraints on the technological autonomy of its member countries by limiting their ability to impose data localization, require source code disclosure, or discriminate against foreign digital products. However, it also grants notable protections by allowing exceptions for legitimate public policy objectives, privacy protection, and law enforcement needs.[133] Heavy reliance on the U.S. market (over 75% of Canadian exports go to the U.S.) creates strategic vulnerabilities and limit Canada's flexibility in trade and procurement decisions. The agreement is scheduled for review in 2026, signaling potential changes that could impact Canada's economic and technological autonomy.[134] (2) The CETA could constrain Canada's autonomy procedurally (by requiring openness and responsiveness), but do not substantively prevent Canada from enacting the technical regulations it deems necessary.[135]
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	No	Canada's domestic and international trade agreements (such as CFTA, CETA) generally require open, non-discriminatory procurement. However, these agreements all contain a "national security exception" (NSE) that allows Canada to exclude a procurement from some

[133] Government of Canada, *Canada-United States-Mexico Agreement (CUSMA) - Chapter 19 - Digital Trade*, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=eng

[134] Gillies, R. (October 2025), *Prime Minister Mark Carney says Canada will double its non-US exports as Canadians can't rely on US*, https://www.msn.com/en-us/news/other/prime-minister-mark-carney-says-canada-will-double-its-non-us-exports-as-canadians-cant-rely-on-us/ar-AA1P0dim?ocid=BingNewsSerp

[135] Government of Canada, *Text of the Comprehensive Economic and Trade Agreement – Chapter four: Technical barriers to trade*, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/04.aspx?lang=eng

		or all trade agreement obligations if necessary to protect its essential security interests.[136] GoC uses legal, policy, and contractual instruments to ensure compliance with Canadian privacy, security, and disclosure requirements. Contracts include standardized security clauses, access restrictions, and incident reporting obligations.[137]
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose restrictions on origin of the funds and the manner in which they are invested?	Yes Examples: (1) Scientific Research and Experimental Development (SR&ED) tax incentives (2) Strategic Innovation Fund	(1) SR&ED tax credits are only available for R&D work performed in Canada. This incentivizes Canadian businesses (and foreign businesses with Canadian operations) to conduct research, development, and innovation activities within Canada's borders.[138] (2) The SIF is designed to attract and anchor high-value investment in Canada, including from global technology leaders, but with conditions that ensure Canada gains lasting benefits (e.g., local R&D, manufacturing, talent development, and sometimes IP retention). The fund is also used to encourage foreign multinationals to build or expand Canadian operations, but not to simply subsidize foreign activity with no Canadian benefit.[139]

[136] Government of Canada, *DAOD 3016-0, National Security Exception Under Trade Agreements* (April 2021), https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/3000-series/3016/3016-0-national-security-exception-under-trade-agreements.html
[137] Government of Canada, *Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada* (October 2025), https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html
[138] Government of Canada, *Scientific Research and Experimental Development (SR&ED) tax incentives* (January 2025), https://www.canada.ca/en/revenue-agency/services/scientific-research-experimental-development-tax-incentive-program.html
[139] Government of Canada, *Strategic Innovation Fund* (October 2025), https://ised-isde.canada.ca/site/ised/en/programs-and-initiatives/strategic-response-fund/strategic-innovation-fund

Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?	Yes Example: Canada rescinds digital services tax to advance broader trade negotiations with the U.S. (2025).	The Canadian government, led by Prime Minister Mark Carney, decided to cancel its digital services tax (DST) on tech giants (mainly large U.S. multinationals) in order to bring the U.S. back to the negotiating table for a broader trade agreement. The first payment of the 3% DST was scheduled for June 30, 2025, on revenues earned in Canada from 2022 to 2024. This example shows that foreign interference, specifically from the U.S., has directly altered Canada's legislative priorities on data and innovation by forcing the cancellation of the digital services tax, a move widely seen as undermining Canadian sovereignty in the digital domain.[140]
Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?	Yes An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts ("Bill C-8") An *Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other*	Bill C-8, if adopted in its current form, will enact the *Critical Cyber Systems Protection Act* ("CCSPA") to establish a comprehensive framework for the protection of "critical cyber systems" in key sectors such as banking, telecommunications, energy, transportation, nuclear, and clearing and settlement systems. It will simultaneously amend the *Telecommunications Act*, making the security of Canada's telecommunications system a central policy objective.[141] In particular, if the Governor in Council believes on reasonable grounds that it is necessary to do so to secure the Canadian telecommunications system against any threat, including that of interference, manipulation, disruption or degradation, the Governor in Council may, by order and after consultation with the persons the Governor in Council considers appropriate,

[140] Roy, J.-H. (July 2025), *Retrait de la taxe sur les services numériques - De nombreuses voix s'élèvent contre Ottawa à la suite de l'annulation de la taxe sur les services numériques*, La Presse, https://www.lapresse.ca/affaires/retrait-de-la-taxe-sur-les-services-numeriques/capitulation-ou-defense-strategique/2025-07-01/retrait-de-la-taxe-sur-les-services-numeriques/carney-a-decide-de-plier.php

[141] Government Bill (House of Commons) C-8 (45-1) - An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts - Parliament of Canada

	related security measures (“Strong Borders Act”) (“Bill C-2”)	(a) prohibit a telecommunications service provider from using all products and services provided by a specified person in, or in relation to, its telecommunications network or telecommunications facilities, or any part of those networks or facilities; or (b) direct a telecommunications service provider to remove all products provided by a specified person from its telecommunications networks or telecommunications facilities, or any part of those networks or facilities. In June, 2025, as its first major legislative initiative, the new federal government introduced Bill C-2, called the “Strong Borders Act”[142]. Parts 14-16 of the bill included a number of provisions dealing with so-called “lawful access”, including: ● a power for a range of law enforcement and governmental agencies to require service providers to provide certain customer information, without obtaining a warrant; ● much broader powers for judicial production and search orders applicable to service providers based on a reasonable grounds to suspect standard; ● specific powers for collection, use, and disclosure of personal information without consent for the purpose of “detecting or deterring money laundering, terrorist activity financing or sanctions evasion”; ● a mechanism for Canadian law enforcement to seek information from foreign service providers; and ● a mechanism to facilitate enforcement of requests for production of transmission data or subscriber information, which seems to have been designed to enable Canada to implement the Second Additional Protocol to the Budapest Convention (sometimes called the “2AP”).

[142] C-2 (45-1) - LEGISinfo - Parliament of Canada

		Canada has signed the 2AP, but not ratified it. The government has not been particularly transparent about its intentions relating to the 2AP. However its underlying intention is to facilitate access by law enforcement in one member state to subscriber information held by a service provider in another member state. Civil society groups (particularly including the Citizen Lab) and the OPC have raised concerns that the 2AP could undermine or conflict with constitutionally-mandated protections of personal information in Canada. Additionally, other parts of the Bill provide for narrower information sharing mechanisms for government departments and agencies. These are relatively unlikely to directly affect a private service provider. Bill C-2 triggered some vocal criticism, including in relation to Part 15. (But also on other issues relating to proposed changes to immigration law, which is not relevant to this analysis.) In response, the government introduced Bill C-12, which replicates most of Bill C-2, but leaves out Parts 14-16 (and a few other unrelated items). Its stated goal was to facilitate quick passage of the immigration and border-related parts of the legislation. However, Bill C-2 was not withdrawn and a group of Ministers and Liberal MPs recently held a press conference calling for swift passage of the original C-2, with particular reference to the lawful access provisions. This makes it difficult to assess the government's legislative strategy or priorities. Finally, the federal government has also indicated that it intends to update Canadian federal data protection (privacy) laws and to introduce new AI legislation.

France

Bertrand Cassar, La Poste, Paris
Emmanuelle Mignon, August Debouzy, Paris
Gilles Rouvier , Lawways Avocats, Paris
Mathilde Lécaillon, Lawways Avocats, Paris
Grimaud Valat, Duclos, Thorne, Mollet-Viéville & Associés (DTMV), Paris,

Executive summary

The main concerns regarding France's technological autonomy are twofold: on the one hand, threats to cybersecurity and the risk that malicious States could seriously compromise the country's functioning and the satisfaction of its population's basic needs; on the other hand, the growth and investment deficit that prevents France from remaining at the right technological level, if not catching up, and makes it dependent in many areas on foreign technologies and capital.

This dependence is now increasingly visible at the level of core digital infrastructures: a significant share of the large-scale data centres and AI computing facilities being built in France are financed and controlled by non-European investors. At the Paris AI Action Summit in February 2025, President Macron announced around €109 billion[143] of mainly private investment in AI, including up to €50 billion from the United Arab Emirates for a 1-gigawatt AI campus and €20 billion from the Canadian fund Brookfield for a hyperscale data centre in Cambrai, alongside multi-billion projects by American cloud and colocation providers such as Amazon, Digital Realty and Equinix. France is trying to close its infrastructure gap partly by relying on non-European capital and operators, which further entrenches its vulnerability. Moreover, when French companies do succeed in AI, a substantial share of their equity quickly ends up in the hands of non-European investors: Mistral AI, for instance, has raised several billion euros since 2023 from US venture capital funds such as Lightspeed, Andreessen Horowitz, General Catalyst, Index Ventures and DST Global, as well as global tech players like NVIDIA, and is currently negotiating an additional $1 billion equity round with Abu Dhabi's sovereign fund MGX.[144][145][146]

While France has had real industrial successes (Mistral AI in the field of AI, Scaleway in the field of cloud computing, Outscale in the field of sovereign cloud computing, Orange in the field of cybersecurity, FranceConnect for digital identity management), and while it retains the ability to train top-level engineers, these successes alone cannot make up for the lack of private investment, particularly in the areas of servers, telecoms, and chips. Like many European countries, France also faces difficulties in accessing rare earths.

Over the last decade, public policies and private initiatives have largely prioritised software, algorithms and the creation of "European champions" in AI and cybersecurity, while under-investing in the underlying physical layers: semiconductor manufacturing, GPU production, high-capacity data centres and energy-intensive network infrastructure. France is emerging as a producer of code and digital services that rely on hardware, networks and

[143] https://www.info.gouv.fr/actualite/ia-une-nouvelle-impulsion-pour-la-strategie-nationale
[144] https://mistral.ai/news/mistral-ai-raises-1-7-b-to-accelerate-technological-progress-with-ai /
[145] https://www.reuters.com/technology/mistral-talks-with-vc-firms-mgx-raise-funds-10-billion-valuation-ft-reports-2025-08-01
[146] https://www.implicator.ai/frances-ai-champion-turns-to-gulf-capital-in-race-against-silicon-valley/

hyperscale facilities that are designed, manufactured or financed abroad, limiting the effective scope of its technological autonomy.

In terms of regulation, France relies on the extensive European legislative arsenal and has also adopted effective national legislation such as the anti-Huawei law and foreign investment controls. However, there is a glaring imbalance between excessive regulation and insufficient private capital, which the State is attempting to address with public subsidies that are not always effective and increase the debt. While there have been attempts to guard against extraterritorial legislation, the real cause of its effectiveness, which is economic, is difficult to address in this context.

Defining Technological Sovereignty	
How is technological sovereignty defined in your jurisdiction? What are the most important factors considered? Examples of Factors: Political Social Dependency perspective IT Infrastructure Legislative perspective (various levels)	French law does not provide for a formally established legal definition of "*technological sovereignty*." Public authorities generally employ this concept in a way that converges with, or is closely related to, the notion of "*digital sovereignty,*" which is not defined by law either. In this regard, the French Senate has defined digital sovereignty as "*the State's ability to act within cyberspace*," which entails, on the one hand, "*an autonomous capacity for assessment, decision-making, and action in cyberspace*," and, on the other hand, control over networks, electronic communications, and data.[147] In a 2021 information report, the National Assembly stated for its part that "*Digital sovereignty constitutes, first and foremost, a strong political ambition - that of achieving strategic autonomy for France and Europe in the field of digital equipment and technologies*."[148] In its analysis, the French Court of Accounts emphasizes that digital sovereignty cannot be assessed in isolation: it must also be understood in relation to other digital powers. A State's ability to maintain its autonomy of assessment, decision-making, and action within cyberspace necessarily requires taking into account - and, at times, standing in opposition to - the competing sovereignties of third countries.[149] The French Council of State shares this analysis, notably in light of the economic weight of Big Tech companies.[150] A summit on European digital sovereignty was held in Berlin on 18 November 2025, bringing together more than 900 participants from the 27 EU Member States. France and Germany presented concrete measures in seven strategic areas to strengthen competitiveness and

[147] Report No. 7 issued on behalf of the Senate's Committee of Inquiry and registered on 1 October 2019 entitled *"The Duty of Digital Sovereignty."*
[148] Report No. 4299 issued by the National Assembly's Information Mission and registered on 29 June 2021 entitled *"Building and Promoting National Digital Sovereignty."*
[149] Final Observations Report of the Court of Accounts No. S2025-1479 deliberated on 11 September 2025 on *"The Sovereignty Challenges of the State's Civil Information Systems.":* "*This requires not allowing fundamental choices to be dictated by third parties, especially given that the dominant players in the digital sector are American companies. This capacity is also threatened by the growing development of extraterritorial legislation*."
[150] 2024 Annual Study of the Council of State, entitled *"Sovereignty."*

	reduce Europe's technological dependencies. A key element of the summit was the launch of a Franco-German working group dedicated to defining European digital sovereignty, which will work in particular to establish a common definition of European digital services and to design sovereignty indicators in key sectors (cloud, AI, cybersecurity), with the results to be presented to the Franco-German Ministerial Council in 2026.[151] Considering all these definitions and the various public reports on the matter, the core issue lies in France's economic capacity to generate growth in order to stimulate investment and technological innovation, in maintaining independence from other States, as well as in the French State's ability to remain autonomous and in control of the digital tools it employs.	
Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?	Yes - French Government's Press Release[152] - Law of 21 May 2024 *on Securing and Regulating the Digital Space*[153]	In 2021, the French Government presented a national Cloud strategy, updated in 2023,[154] with the ambition of making cloud technology a key component of France's digital sovereignty. The strategy is structured around four key pillars: For the most sensitive processing and data, or data whose compromise would undermine the proper functioning of the State, the French State has developed two *internal cloud* services based on OpenStack open source technology and monitored by the Ministry of the Interior (PI cloud), associated with a "restricted distribution" security level, and by the Ministry of Finance (NUBO cloud), associated with the SecNumCloud standard (ANSSI reference qualification). It also exists an internal cloud meeting the specific needs of the Defense; The *"Cloud de confiance"* or *Trusted Cloud* label is designed to allow French compagnies and public bodies to access state-of-the-art cloud services while guaranteeing optimal data protection. This framework relies on the *SecNumCloud* certification scheme, granted by the *National Cybersecurity Agency of France (ANSSI).* If the computer system or application

[151] Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe

[152] Government Press Release No. 1002 17 May 2021 "*The Government Announces Its National Cloud Strategy*."

[153] Law No. 2024-449 of 21 May 2024 *on Securing and Regulating the Digital Space*

[154] Circular No. 6282/SG of 5 July 2021 *concerning the State's Doctrine on the Use of Cloud Computing* https://www.legifrance.gouv.fr/download/pdf/circ?id=45446

		processes State's data, whether personal or not, that is of a specific sensitivity and whose breach is likely to cause harm to public order, public safety, human health and life, or the protection of intellectual property, the commercial cloud offering selected must comply with the SecNumCloud certification (or a European certification guaranteeing at least an equivalent level, particularly in terms of cybersecurity) and be immune to any unauthorized access by public authorities of third countries; The "*Cloud au centre*" or *Cloud at the center* policy, which consists in adopting a doctrine within the French administration aimed at accelerating the digital transformation of public services; An industrial policy directed at funding and supporting French cloud innovation through a range of dedicated national programs and investment plans. Furthermore, Law No. 2024-449 of 21 May 2024 *on Securing and Regulating Digital Space* includes several key provisions relating to cloud services. These notably concern the regulation of data transfer and migration fees, the limitation of cloud credits (commercial vouchers) to a maximum duration of one year, and the obligation for cloud services to ensure interoperability. More recently, as part of the *France 2030 Plan*, the French Government adopted a *Cloud Acceleration Strategy* structured around five key pillars:[155] Reinforcing France's digital sovereignty through the development and adoption of a *Trusted Cloud* that protects users' data in accordance with European values; Promoting research, development, and innovation in emerging cloud-related fields with strong value-creation potential (including edge computing, artificial intelligence, and 5G), and supporting French technological initiatives to enhance national cloud autonomy; Accelerating the State's digital transformation;

[155] General Directorate for Enterprise published on 18 October 2024 "*France 2030: Cloud Acceleration Strategy*."

		Driving the greening and sustainability of the cloud industry; Advancing cloud-related education and skills development. The *France 2030* Plan, endowed with €54 billion over five years (all sectors combined), aims in particular to "*bring about the lasting transformation of key sectors of [French] economy.*"[156]
AI and Technology Sovereignty policy		
Has your jurisdiction published a national technology sovereignty policy?	Yes - National Recovery and Resilience Plan[157] - France Relance Plan[158] - France 2030 Plan[159]	The objective of technological sovereignty has been firmly integrated into several overreaching national strategies. Since 2020-2021, the French Government has launched large-scale investment programs (France Relance followed by France 2030) explicitly designed to strengthen France's technological and industrial sovereignty across strategic sectors. In essence, France's approach consists of a coherent framework of coordinated sectoral strategies (in areas such as cloud, AI, cybersecurity, quantum computing, and microelectronics) backed by significant public investment to guarantee the technological autonomy of both France and Europe. The *France Relance* plan (2020) included a component dedicated to "*technological sovereignty and resilience*," with targeted investments to develop national capacities (for example, support for the electronics sector, cloud computing, and digital health.) This focus was further reinforced with the *France 2030* plan (launched at the end of 2021), endowed with €54 billion through to 2030, which explicitly aims to position France as a leader in future technologies in order to "*preserve its technological and industrial sovereignty*."

[156] French Government's website published on 13 October 2023 "*France 2030: An Investment Plan for France.*"
[157] French Government's website published on 15 September 2025 "*France's National Recovery and Resilience Plan*."
[158] French Government's website published on 13 October 2023 "*France 2030: An Investment Plan for France.*"
[159] French Government's website published on 13 October 2023 "*France 2030: An Investment Plan for France.*"

		Under the *France 2030* framework, several national technology strategies have been published, each incorporating a sovereignty dimension. This is notably the case of the *National Artificial Intelligence Strategy*[160] (see next section), which sets the objective of "*preserving and consolidating France's economic, technological, and political sovereignty*" in the field of AI. Similarly, the *National Cybersecurity Strategy*[161] (2021) focuses on developing French capabilities in digital security to reduce dependencies, while the *National Quantum Strategy*[162] (2021) aims to position France among the leading nations mastering quantum technologies in a sovereign manner. Each of these roadmaps contributes to the broader policy objective of achieving technological autonomy.
Does your jurisdiction have a published national AI strategy/policy?	Yes - Villani Report[163] - French Government Publications[164],[165] - Court of Accounts Report[166]	France has developed and published a *National Artificial Intelligence Strategy*. Initially launched in 2018 following the *Villani Report*, prepared as part of a mission commissioned by the French Prime Minister, this strategy has been implemented in successive phases and was renewed and strengthened in 2021, and again for the 2023-2025 period. Phase 1 (2018-2022) aimed to provide France with world-class research capabilities. Backed by €1.5 billion in funding, this strategy is based on four main areas: strengthening a research and experimentation ecosystem, implementing a policy of opening up public and private data,

[160] General Directorate for Enterprise published on 7 February 2025 "*National Artificial Intelligence Strategy.*"
[161] General Directorate for Enterprise published on 19 November 2024 "*National Cybersecurity Strategy.*"
[162] General Directorate for Enterprise published on 7 July 2023 "*National Quantum Strategy.*"
[163] *Villani Report*, submitted on 28 March 2018 following a mission commissioned by Prime Minister Édouard Philippe and conducted as a parliamentary assignment from 8 September 2017 to 8 March 2018 entitled *"Giving Meaning to Artificial Intelligence: For a National and European Strategy."*
[164] General Directorate for Enterprise published on 20 September 2024 *"France 2030: National Artificial Intelligence Strategy."*
[165] French Government's website published on 13 October 2023 "*Artificial Intelligence: A New Momentum for the National Strategy*."
[166] Thematic Public Report of the Court of Accounts on Public Entities and Policies published in November 2025 entitled *"The National Artificial Intelligence Strategy."*

		developing a public and private funding strategy to accelerate France's presence in international competition, and considering the terms of a political and ethical debate on artificial intelligence, including algorithm transparency and non-discrimination. It resulted in the establishment of a network of Interdisciplinary Institutes for Artificial Intelligence, 180 Chairs of Excellence, and 300 PhD programs, as well as the deployment of the Jean Zay high-performance supercomputer. Phase 2 (2022-2025) focuses on mainstreaming AI technologies within the national economy through three key drivers: advancing education and research, supporting cutting-edge AI solutions, and bridging the gap between supply and demand for AI. This second phase is supported by a budget of €2.22 billion (including €1.5 billion in public funding and €506 million in private co-financing), aims to transform scientific and research potential into economic success. This strategy is based on three key objectives: developing national skills (training and talent), making France a leader in the fields of embedded, frugal and trusted AI, and accelerating the spread of AI in the economy (by supporting the development of sovereign and interoperable platforms in data science, machine learning and robotics). The strategy also encourages the pooling of data, both inter- and intra-sector, as seen in the agriculture (AgDataHub), logistics (IACargo) and automatic voice processing (VoiceLab) sectors. Public funding comes mainly from the Future Investment Programme (PIA4) and France 2030. In February 2025, the French Government unveiled the third phase of its National Artificial Intelligence Strategy, reaffirming France’s long-term ambition to foster world-class AI capabilities while strengthening its technological sovereignty. This phase notably seeks to increase the attractiveness of France and its high-level innovation ecosystem, and to leverage artificial intelligence to serve public policy objectives and improve administrative performance. On 9 February 2025, ahead of the Summit for AI Action, which brought together international

		experts and decision-makers, the President of the Republic announced that €109 billion in private investment would be directed toward artificial intelligence in France over the next few years. Under the *France 2030* plan, the AI training component aims to support the development of artificial intelligence in France through a highly skilled and sizeable workforce. Financed with €360 million, the *"AI Clusters"* program seeks to create a "*French MIT*." Nine training and excellence hubs in AI are being established, with the 2030 objectives of: • training 100,000 people; • placing at least one center of excellence among the world's leading institutions. The funding of new *AI Chairs of Excellence* is intended to further strengthen France's attractiveness, enhance the university and engineering school network, and expand training opportunities while encouraging the return of French talent. A *"Choose France for Research"* unit will also be launched to assist talented researchers wishing to establish themselves in France. The Government aims to mainstream the use of artificial intelligence across public administration to enhance the quality and effectiveness of public service delivery. Interministerial efforts to implement AI within the public sector will be coordinated by the Ministry for Public Action, Civil Service and Administrative Simplification. A deployment plan for generative AI tools will provide civil servants with secure and competitive AI assistants. Teachers, magistrates, and law enforcement officers will be equipped with technologies designed to improve productivity and administrative efficiency.
Does your jurisdiction have a published AI compute or cloud strategy/policy?	Yes - Interministerial Committee on	Reinforcing computational capacities constitutes a key element of France's overall technological strategy, especially to support artificial intelligence and cloud-related requirements.

	Artificial Intelligence [167] - AI Summit in France[168] - Court of Accounts Report[169]	While no specific strategy is dedicated solely to high-performance computing, France continues to invest heavily in supercomputers and *High-Performance Computing (HPC)* infrastructure under its broader AI and digital transformation programs. During Phase 1 of the National AI Strategy, France funded the deployment of the Jean Zay supercomputer (operated by the CNRS at IDRIS), primarily dedicated to artificial intelligence research. Commissioned in 2019, Jean Zay has undergone several successive upgrades, increasing its power to more than 125 petaflops by 2023. It constitutes a key strategic asset, allowing French researchers and enterprises to train AI models using world-class computing resources, without depending exclusively on GAFAM cloud infrastructures. Through the EuroHPC initiative (the European Joint Undertaking for High-Performance Computing), France co-funds the acquisition of even more powerful supercomputers. A flagship project is the construction of the future French exascale supercomputer, Alice Recoque, hosted by the CEA, which will be among the very first of its kind in Europe. Expected to be operational by 2025, Alice Recoque will deliver unprecedented computing power, equivalent to 25,000 high-end GPUs. In parallel, another supercomputer, Adastra (located at CINES), was inaugurated in 2022 and ranks among the world's most energy-efficient systems. These investments form part of both the national and European strategies for high-performance computing, aiming to strengthen strategic autonomy in processing large-scale data and advancing cutting-edge artificial intelligence. Alongside conventional HPC initiatives, France's strategy encourages the expansion of sovereign

[167] Interministerial Committee on Artificial Intelligence held as part of the *Summit for AI Action* on 6 February 2025 entitled *"Making France a Global AI Power."*
[168] Contribution from the Presidency of the French Republic as part of the *Summit for AI Action* on 11 February 2025 entitled *"Making France a Global Power in Artificial Intelligence."*
[169] Thematic Public Report of the Court of Accounts on Public Entities and Policies published in November 2025 entitled *"The National Artificial Intelligence Strategy."*

		cloud computing capacities for the private sector. The development of nationally certified cloud solutions (SecNumCloud) and decentralized computing infrastructures is part of broader efforts to ensure that both public and private actors have access to secure computing capabilities within France.
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks related to technological sovereignty?	Yes, very lively - i.e. all sources mentioned above	In France, the debate on digital sovereignty is highly active and has become a major political issue. In recent years, there has been a proliferation of positions, reports, and initiatives on the subject, both at the parliamentary level (reports of the Senate and the National Assembly between 2019 and 2021) and at the governmental level (digital sovereignty strategies integrated into the Recovery Plan, the France 2030 Plan official speeches, etc.). The Council of State devoted its 2024 Annual Study to the theme of sovereignty, while the Court of Accounts regularly publishes major reports concerning artificial intelligence. Within the corporate and public sectors alike, there has been a growing awareness of sovereignty-related challenges and an increasing number of measures addressing them. According to a recent survey, 65% of French business leaders view digital sovereignty as a key strategic issue for their organizations.[170] In 2025, France demonstrated the priority it placed on digital sovereignty through three major initiatives. First, the creation of the Digital Sovereignty Observatory in July 2025, designed to measure technological dependencies and map risks. Next, the AI Summit, which attracted €109 billion in investment, highlighting France's strengths in infrastructure and carbon-free energy. Finally, the call for projects 'Strengthening the Cloud Services Offering' launched on 14 April 2025, as part of France 2030, to support strategic technologies (cloud, AI, cybersecurity, quantum) and develop a competitive European offering to rival non-European solutions[171]. As abovementioned, on 18 November 2025 in Berlin, the Franco-German Summit on European Digital

[170] https://www.oodrive.com/fr/blog/secnumcloud/souverainete/souverainete-numerique/
[171] Council of Ministers meeting of 12 June 2025. Digital sovereignty

		Sovereignty launched a working group dedicated to defining European digital sovereignty and creating sovereignty indicators in strategic sectors (cloud, AI, cybersecurity), with results expected in 2026.[172]
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	Yes Mistral BLOOM LightOn Lyra-fr LUCIE	Mistral:[173] models developed by the Paris-based startup Mistral AI (French law entity); Sector: Private BLOOM (BigScience/HuggingFace/CNRS/GENCI):[174] model resulting from the BigScience project, largely coordinated from France and trained on the public supercomputer Jean Zay with strong support from CNRS/GENCI. Sector: mainly public/academia (with a private industrial lead) LightOn: Lyra-fr foundation model Sector: private Lucy (LINAGORA and the OpenLLM-France):[175] open source foundation model. Sector: private with public support
Does your jurisdiction have national AI research centres of excellence?	Yes Examples: INRIA CNRS CEA LIST IA Clusters France 2030	Links to AI research centres of excellence: INRIA: https://www.inria.fr/fr CNRS: https://aissai.cnrs.fr/ CEA LIST: https://list.cea.fr/fr/ IA Clusters: 9 AI Clusters https://anr.fr/actus/details/news/intelligence-artificielle-9-nouveaux-ia-clusters-et-2-nouveaux-laureats-competences-et-metier/
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes	Research: national quantum strategy launched in 2021, budget of around €1.8 billion (Quantum Plan / France 2030) lead: CNRS, CEA, Inria and universities. PEPR Quantique, lead :CEA, CNRS and Inria,

[172] Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe
[173] https://mistral.ai/fr / https://fr.wikipedia.org/wiki/Mistral_AI
[174] https://bigscience.huggingface.co/blog/bloom / https://fr.wikipedia.org/wiki/BLOOM_(mod%C3%A8le_de_langage)
[175] https://lucie.chat/ / https://www.genci.fr/en/news/new-milestone-french-ai-flagship-jean-zay-drive-major-ai-breakthroughs-thanks-record-eviden?utm_source=chatgpt.com

		Infrastructure: national hybrid quantum computing platform (HQI), combining classical supercomputers and quantum machines, operated by CEA / GENCI with French industrial partners. Commercialization: Pasqal[176] : French company that designs neutral-atom quantum processors and commercializes them for industrial use cases. Quandela[177] : develops and sells photonic quantum computers, available via the cloud and, since 2024, selected to equip the EuroQCS-France platform (photonic quantum computer operated by CEA).
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech stack, funding and adoption:	Please rate each component on a five point scale and circle the best option (1 = non-existent; 2 = nascent; 3 = existing but insufficient; 4 = solidly in place; 5 = world leading): AI compute (GPU-equipped) data centres 1 2 3 4 5 Domestically developed AI foundational models 1 2 3 4 5 Existence of large high-value databases in high-value sectors of economic activity 1 2 3 4 5 Availability of funding/financing for commercialization of innovation 1 2 3 4 5 Rates of AI adoption by organizations 1 2 3 4 5 Domestic quantum computing research, development and commercialization 1 2 3 4 5	
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	Yes	Apart from copyright, databases benefit from a specific sui generis right granted to the producer of the database (the person who takes the initiative and bears the risk of the investment). This right applies when there has been a substantial investment (financial, human or technical) in the obtaining, verification or presentation of the contents of the database. The sui generis[178] right allows the producer to prohibit:

[176] https://www.pasqal.com/fr/
[177] https://www.quandela.com/
[178] EU Database Directive (96/9/EC) and French Intellectual Property Code (Articles L.341-1 et seq. CPI)

		the extraction or re-utilisation of all or of a qualitatively or quantitatively substantial part of the contents; and repeated and systematic extractions or re-utilisations of insubstantial parts that conflict with the normal exploitation of the database.
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?	Yes	France has specific statutory TDM exceptions in its Copyright Act (Articles L.122-5 (10°) and L.122-5-3 IPC, from Directive UE 2019/790), including a mandatory exception for scientific research and a general TDM exception (with rightholder opt-out) that can support both research and commercial innovation.
Does your jurisdiction have (1) an open, principle-based notion of "fair use" or (2) a closed, listed exceptions-based notion of "fair dealing"? Do those rules favor national players?	No	France has a closed, exceptions-based "fair dealing" system (no open-ended fair use doctrine), and these rules do not formally favor national players
Have courts in your jurisdiction issued decisions on the application of "fair dealing" or "fair use" in relation to the use of unlicensed data to train AI models (i.e. via screen scraping)?	No	In France, no published court decision has yet ruled on the merits of the lawfulness of using data (protected works or personal data) to train AI systems. In the field of intellectual property, several actions have been brought – in particular the claim filed against Meta before the Paris Judicial Court over the training of LLaMA on protected books – but these cases are still pending.[179] In the field of personal data, it is mainly the CNIL and the European authorities that have taken a stance (formal notices and guidelines on the use of data for AI), and French courts have not, at this stage, handed down any landmark rulings.
Are there any other special exclusivity rights provisions (data ownership in a strict	Yes	France does not recognize a general property right in data. Instead, control over data is organized through specific regimes (database sui generis right,

179 https://www.lemonde.fr/economie/article/2025/03/12/auteurs-et-editeurs-attaquent-meta-pour-violation-du-droit-d-auteur_6579662_3234.html?

sense) in your jurisdiction? Do those rules favor national players?		trade secrets, personal data protection, open data rules and EU data-sharing regulations such as the Data Act and the DGA), but they grant access and use rights rather than full ownership of data.
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: in the public sector? in the private sector?	Examples: a) Public sector: (1) GDPR (2) Rules on National Defense Secrecy (3) SecNumCloud Certification (4) HDS Certification (5) "Blocking Statute" of 1968[180] (6) EU Regulation 2018/1807[181] (7) Data Act[182] b) Private sector: Provisions of public sector also mostly apply	a) In the French public sector, several provisions apply: GDPR governs the transfer of personal data to third countries or international organizations through mechanisms such as adequacy decisions or appropriate safeguards. Rules on National Defense Secrecy define the notion of "*classified information and materials*" covered by national defense secrecy. SecNumCloud Certification establishes the reference framework of requirements applicable to cloud service providers seeking a security certification (security visa). Health Date Hosting (HDS) Certification requires that the physical hosting of health data be carried out exclusively within the territory of a country belonging to the EEA, with reinforced sovereignty and transparency obligations. "Blocking Statute" prevents foreign authorities from obtaining access to sensitive information affecting the Nation's interests (sovereignty, security, essential economic interests, public order) by requiring them to use official channels of judicial or administrative cooperation. EU Regulation 2018/1807 enshrines the free movement of non-personal data within the EU and allows localization restrictions only on grounds of public security. Data Act establishes a framework to facilitate access to and sharing of data generated by connected products. It gives users greater control while protecting the interests of manufacturers and fostering innovation within the European Union.

[180] Law No. 68-678 of 26 July 1968 *on the Communication of Documents and Information of an Economic Commercial Industrial Financial or Technical Nature to Foreign Natural or Legal Persons*
[181] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 *on a framework for the free flow of non-personal data in the European Union*
[182] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 *on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828* "*Data Act*"

		b) In the French private sector, there is no general rule requiring "*France-only*" data hosting. Sovereignty and localization constraints for private sector primarily stem from (i) EU regulations on data transfers, (ii) sector-specific regulatory regimes, and (iii) cybersecurity or contractual requirements imposed on service providers (cloud and IT). For example, *HDS (Health Data Hosting)* certification is mandatory for any organization, public or private, that hosts health-related data. Likewise, the *SecNumCloud* label, while not compulsory for private entities, is recommended by *ANSSI* for the protection of sensitive information and is frequently required in public tenders or in situations involving potential extraterritoriality risks. In addition, European instruments such as the *General Data Protection Regulation (GDPR)* and the *Regulation on the Free Flow of Non-Personal Data* are fully applicable. The "Blocking statute" also applies prohibiting private individuals or legal entities from communicating directly with foreign public authorities sensitive information affecting the Nation's interests, along with documents or information of an economic, commercial, industrial, financial, or technical nature that may be used as evidence in foreign judicial or administrative proceedings.
What are special classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?	- French Defense Code[183] - Interministerial General Instruction No. 1300[184] - Circular No. 6282/SG[185]	The legal framework for data classification is defined in the French Defense Code, which determines the various levels of confidentiality (restricted distribution, secret, top secret) together with Interministerial General Instruction No. 1300, detailing the regulations for the protection of classified defense information. The Interministerial General Instruction No. 1300 notably provides that information systems processing classified information must be

[183] Articles R.2311-1 to R.2311-9 of the French Defense Code
[184] Interministerial General Instruction No. 1300 *on the Protection of National Defense Secrets* issued by the Ministerial Order of 9 August 2021
[185] Circular No. 6282/SG of 5 July 2021 *concerning the State's Doctrine on the Use of Cloud Computing*

		accredited and secured using means approved by the National Cybersecurity Agency of France (ANSSI), in order to ensure that no unauthorized person - and no foreign State - can gain access. Consequently, classified information may only be hosted on secure French or allied sites or networks (under reciprocal security agreements). For instance, a Secret-Défense document may neither transit through nor be stored on a foreign public cloud. Even the "*Restricted Distribution*" marking, although it does not constitute a formal level of classification, imposes specific constraints: documents bearing this designation must only be accessible to individuals with a need-to-know basis, and their preparation must take place in premises providing adequate security conditions that prevent access by unauthorized persons. In short, any data covered by defense secrecy or national security obligations must remain under France's exclusive control, based on the combined legal authority of the Criminal Code (protection of classified information) and the regulatory instruments implementing it - namely, the Defense Code and the Interministerial General Instruction No. 1300, approved by ministerial decree.
What are the most notable cross-border data transfer restrictions in your jurisdiction?	- Articles 44 and following of GDPR[186] - "Blocking Statute" of 1968 and Decree No. 2022-207 of 18 February 2022[187]	In 2025, restrictions on cross-border data transfers under French jurisdiction are mainly framed by the GDPR and its recent implementing developments, subject to reinforced supervision by the *French Data Protection Authority (CNIL)*. Under the GDPR, personal data may not be transferred to third countries unless adequate safeguards are implemented or the recipient country has been recognized as providing an "*adequate level of protection*." In all other cases, such transfers are considered unlawful.

[186] Articles 44 and following of the GDPR which govern international data transfers

[187] Law No. 68-678 of 26 July 1968 *on the Communication of Documents and Information of an Economic Commercial Industrial Financial or Technical Nature to Foreign Natural or Legal Persons* and Decree No. 2022-207 of 18 February 2022

		Furthermore, the “Blocking statute” prohibits any person, whether natural or legal, from communicating directly with foreign public authorities sensitive information affecting the Nation’s interests, along with documents or information of an economic, commercial, industrial, financial, or technical nature that may be used as evidence in foreign judicial or administrative proceedings. This “Blocking Statute”, strengthened by a decree and ministerial order in 2022, requires foreign authorities or requesting parties to use formal international cooperation procedures to obtain sensitive information. Failure to do so may place the French company concerned in a situation of illegality under French law.
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?	Examples: - (1) Order of the French Council of State[188] - (2) Formal Notice by the CNIL in the “Google Analytics” Case[189] - (3) CNIL Practical Guide[190]	Order of the French Council of State: Following the Schrems II ruling, the Council of State, in summary proceedings concerning the Health Data Hub, held that the “*no transfer*” of data to the United States could rely on an adequacy decision and that any transfer to a service provider subject to US law might breach Articles 44 et seq. GDPR. Fearing potential transfers of personal data to the United States, a coalition of associations and trade unions petitioned the interim relief judge of the Council of State to order the urgent suspension of the Health Data Hub platform. The judge held that the personal data hosted in the Netherlands under a contract with Microsoft could not lawfully be transferred outside the European Union. Although the possibility that US intelligence agencies might seek access to this data could not be fully excluded, such a risk did not, in the immediate term, warrant suspension of the platform. Nonetheless, the judge ordered the adoption of special safeguards, subject to oversight by the CNIL. CNIL Formal Notice - Google Analytics: Following complaints filed by the NOYB association after

[188] CE 13 October 2020 No. 444937

[189] Formal Notice published by press release on 10 February 2022 concerning the use of Google Analytics by French website operators

[190] CNIL Practical Guide on Conducting “*Data Transfer Impact Assessments*” published in January 2025

		the Schrems II ruling, the CNIL issued a landmark decision concerning a French website using Google Analytics. The authority found that the data of the site's visitors were being transferred to the United States via Google Analytics, in breach of Articles 44 et seq. of the GDPR. In its statement, the CNIL stressed that such transfers were unlawful due to the absence of sufficient safeguards and gave formal notice to the website operator to comply within one month - "*if necessary, by ceasing to use the Google Analytics functionality (in its current conditions) or by adopting a tool that does not involve transfers outside the EU.*" In other words, the CNIL required either discontinuing the use of Google Analytics or replacing it with a European alternative, as long as data continued to be exported to the US without adequate protection. This public decision was historic, as it was the first time the CNIL had formally declared data transfers to the United States illegal in connection with a commonly used service. CNIL Data Transfer Impact Assessment Guide: The CNIL has recently released a practical guide on conducting Data Transfer Impact Assessments, designed to assist organizations that transfer personal data beyond the European Economic Area (EEA).
Information Security Laws for Critical Infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Yes	France has specific information security regimes for critical infrastructure (OIV under the Military Programming Law and essential/important entities under NIS2), imposing enhanced cybersecurity, governance and incident-reporting obligations on both state-owned and private operators. France is subject to the EU framework, including the Critical Entities Resilience Directive (EU) 2022/2557, the EU Cybersecurity Act (Regulation (EU) 2019/881), and sector-specific instruments such as DORA for financial services. These instruments apply across the EU and do not formally favour national players, but they drive a high and relatively

		harmonised level of information security for critical infrastructure operators in Europe. EU AI Act adds an additional layer of obligations for the use of AI in critical sectors.
In your jurisdiction, can directors and officers be held accountable for not diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?	In theory yes	Under general directors' duties and sectoral regulation (e.g. cybersecurity, operational resilience, critical infrastructure rules), directors and officers may be held accountable – ex post – if a failure to identify and mitigate concentration risk amounts to a breach of their general duty of care or of specific regulatory obligations.
Lawful Access (Legal Access to Data without Consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?	For French authorities: yes - Criminal Procedure Code[191] - Postal and Electronic Communications Code[192] - Internal Security Code[193] For foreign authorities: yes, but under strict conditions - *Directive on the European Investigation Order*[194]	French legislation allows judicial and intelligence authorities to access personal data held by private entities (including internet service providers, hosting companies, and cloud operators) without requiring the consent of the individuals concerned. In criminal proceedings, the Criminal Procedure Code empowers prosecutors and judicial police officers to requisition data from third parties without notifying the data subject. Furthermore, the Postal and Electronic Communications Code requires operators to retain specific categories of metadata (identifiers, geolocation data, connection records) for potential transmission to the competent authorities. In the field of intelligence gathering, the Internal Security Code enables intelligence agencies to collect and analyze connection data, and in some

[191] Articles 60-1 and 77-1-1 of the Code of Criminal Procedure
[192] Article L.34-1 of the Postal and Electronic Communications Code
[193] Article L.851-1 and following of the Internal Security Code
[194] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 *on the European Investigation Order in criminal matters*

	- GDPR	cases intercept communications in real time, without prior consent. Overall, French law allows the access to personal data for both criminal justice and national security purposes without the prior consent of the data subjects. Concerning foreign authorities, a distinction must be made between EU foreign authorities and out of EU foreign authorities: For European judicial authorities, the European Investigation Order enables an authority in one EU Member State to directly and easily request the gathering and transmission of evidence by another Member State within the framework of criminal proceedings. he requested Member State is in principle obliged to respond and may only refuse the request in very limited circumstances; French laws do not grant foreign authorities out of EU any direct right of access. On the contrary, the legal framework requires that requests originating from third countries be channeled through formal cooperation mechanisms or international treaties. GDPR, which is directly applicable, provides in its article 48 that no decision by a foreign public authority requiring the disclosure of personal data may be recognized or enforced in France unless it is based on an international agreement in force, such as a mutual legal assistance treaty.
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a “collect all” regime) under such lawful access regime?	No	Bulk data collection or transfer is not permitted under ordinary legal frameworks for data access in France, and this prohibition has been consistently reaffirmed by the Court of Justice of the European Union. In criminal proceedings, only specific and proportionate requests for access to data are allowed, while indiscriminate or generalized data collection remains prohibited. However, in the field of intelligence, broader measures may exceptionally be authorized for national security purposes (for example, through automated data processing or international surveillance programs) but such operations must receive prior approval from the Prime Minister

		and are subject to oversight by the *National Commission for the Control of Intelligence Techniques* (CNCTR). The generalized retention of connection data may only be authorized on a temporary basis where a serious threat to national security exists (which can be fairly easily recognized).
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?	Yes, under specific circumstances - Code of Criminal Procedure - Internal Security Code	In France, government access to personal data is subject to strict judicial control. During criminal investigations, the public prosecutor may directly obtain information from third parties, such as businesses, network operators, or public bodies without a judicial warrant, but under the prosecutor's hierarchical oversight. However, intrusive investigative measures, including telephone tapping or access to private communications, must be authorized by a judge. Consequently, data access is governed by the principle of proportionality: routine requests are handled by the prosecutor, while measures that seriously interfere with privacy fall within the competence of a judicial magistrate. Outside cases of urgency, any large-scale or indiscriminate collection of data requires the intervention or control of the judicial authority. In the field of intelligence, judicial authorization is not systematically required, but no surveillance technique may be implemented without prior authorization. Such authorization falls within the competence of the Prime Minister, who may grant it only after consulting the National Commission for the Control of Intelligence Techniques.[195] In the absence of such authorization, the implementation of an intelligence technique would amount to a criminal offence. This framework covers all surveillance methods defined by statute and applies to all intelligence agencies empowered to use them. Furthermore, intelligence services are required to comply with a strict authorization procedure: they must substantiate their request, indicate the purpose pursued, and specify the duration of the

[195] https://www.cnctr.fr/controle-prealable

		measure, in order to guarantee effective control over the legality and proportionality of the surveillance.
Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Yes - Budapest Convention on Cybercrime - Regulation (EU) 2023/1543[196]	The framework for the transmission and execution of requests for mutual legal assistance in criminal proceedings is set out in Articles 694 et seq. of the French Code of Criminal Procedure. France is a contracting party to many bilateral and multilateral treaties on mutual legal assistance in criminal matters. These instruments include provisions on extradition, cooperation during criminal investigations, and the transfer of convicted individuals.[197] In this regard, reference may be made to the Budapest Convention on Cybercrime, an international treaty adopted by the Council of Europe on 23 November 2001 in Budapest. Under the auspices of the United Nations, several multilateral conventions containing provisions on international mutual legal assistance in criminal matters have also been concluded. The European Judicial Network website serves as a central access point to all EU instruments governing judicial cooperation in criminal matters (including those related to the European Arrest Warrant and the European Investigation Order). It also provides information on the competent judicial authorities across the Member States. In response to the growing volume and rapid flow of data exchanges, the European Union is developing new legal mechanisms. In 2023, the EU adopted the e-Evidence Package (Regulation (EU) 2023/1543 and the related Directive), which will, from 2026 onwards, allow judicial authorities in one Member State to directly issue an order to a service provider established in another Member State for the disclosure or preservation of electronic evidence.

[196] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 *on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences*

[197] French Ministry of Justice on 20 April 2023, entitled "*European and International Judicial Cooperation*."

		Under French domestic law, treaties or international agreements duly ratified have authority superior to that of ordinary legislation, but they cannot prevail over constitutional principles. France therefore shall ensure, in principle, prior to ratification, that any agreement does not entail unacceptable derogations from fundamental rights. In conclusion, France takes an active part in international cooperation frameworks on lawful access to data while never compromising the protection of its residents' personal data. The agreements in force are designed to reconcile the effectiveness of cross-border investigations with the preservation of fundamental rights: all include safeguard clauses or limitations to ensure that access requests comply with French and European legal standards of proportionality, oversight, and redress.
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation? What is their most notable impact on promoting technological autonomy?	French competition law and EU DMA.	In France, the most important regime is the general EU/French competition law framework (now complemented by the Digital Markets Act), whose main impact on technological autonomy lies in limiting gatekeeper power and keeping digital markets open for European and French innovators, with the DMA in particular imposing ex ante obligations on designated gatekeepers (interoperability of core services, data access and portability, bans on self-preferencing and certain tying/bundling practices, fairer app store and in-app payment conditions, and limits on combining personal data across services) so that smaller EU players can compete and scale without being structurally dependent on a handful of dominant non-European platforms.
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?	Yes	Recent French and EU enforcement has been applied in ways that de facto support technological autonomy, by opening up markets vis-à-vis dominant (often non-EU) platforms. For example: the French Competition Authority fined Apple €150 million over its App Tracking Transparency (ATT) implementation in iOS, finding that Apple abused its dominance in mobile app advertising by imposing asymmetric conditions on third-party apps versus its

		own, thereby harming independent app developers and adtech providers; the Commission has launched DMA non-compliance investigations into Alphabet, Apple and Meta over app-store steering, search self-preferencing and "pay-or-consent" models, and in April 2025 imposed the first DMA fines (Apple €500m, Meta €200m) for anti-steering rules in the App Store and Meta's coercive consent model.
Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes")?	Yes	1. No FTA in France that constrains technological autonomy or enables foreign data access France, through the EU, has no free trade agreement with the U.S[198] and therefore no treaty-based exposure to the CLOUD Act, MLAT-type automatic data transfers, or "Five Eyes" intelligence-sharing obligations. Any U.S. data-access risk is unilateral (CLOUD Act), not based on an FTA. 2. EU FTAs contain *protections*, not constraints All modern EU FTAs (Japan, Canada/CETA, Korea, Singapore, Vietnam, New Zealand, etc.)[199] include: GDPR / Article 16 TFEU carve-outs → EU keeps full autonomy over personal-data regulation; National-security and public-order exceptions → allow restricting foreign tech or cloud providers for sovereignty reasons; No binding commitments on cross-border data flows → unlike U.S.-style FTAs, EU FTAs do not prohibit data-localisation or EU-only requirements; Exclusions for sensitive digital sectors → e.g., cloud, telecom security, audiovisual, public services. These clauses preserve France's ability to impose sovereignty measures (e.g., SecNumCloud requirements, restrictions on 5G suppliers, rules for critical infrastructure). 3. France is not part of any FTA with intelligence-sharing effects France is not in the "Five Eyes";

198 https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en#:~:text=Despite%20the%20US%20being%20the,were%20formally%20closed%20in%202019.

199 https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-10-16-edps-opinion-262025-recommendation-council-authorising-opening-negotiations-digital-trade-agreement-canada_en

		No EU FTA includes obligations that facilitate foreign intelligence access or constrain cybersecurity policy. 4. MLATs exist but do not affect technological autonomy France has MLATs (including with the U.S.), but these are criminal-cooperation treaties, not trade agreements: they do not give foreign authorities rights over cloud-stored data; they do not affect procurement, cloud policy, or digital sovereignty.
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	Yes	France has no "*buy local / buy French*" procurement rule specifically targeting advanced technologies. However, certain provisions of the French Public Procurement Code can *indirectly* apply to technology products when they qualify as supplies, including hardware and embedded software. Article L.2153-1 of the French Public Procurement Code[200] — Allows a preference for EU products over non-EU products for countries not part to EU FTAs or the WTO GPA. Key Limitation: No preference for services (cloud, AI, cybersecurity, software development) EU Public Procurement Directive 2014/24/EU, Art. 18 and related provisions: non-discrimination applies to services, and you cannot exclude or prefer a bidder based on nationality or the origin of a service; GPA/WTO obligations: services are covered by the agreement, and origin-based restrictions are generally prohibited. Article L.2153-2 of the French Public Procurement Code[201] — Applies only to "entités adjudicatrices" (utilities: water, energy, transport, postal sectors) and only to supply contracts. These entities may: Exclude an offer if more than 50% of the products originate from non-EU / non-GPA countries; Grant a preference to products of EU origin. Relevance for advanced technologies: Embedded software in telecom/network equipment is legally treated as a product.

[200] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037703671
[201] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037703675/2025-11-26

		Therefore, telecom, network and cybersecurity equipment may fall under Article L.2153-2. But this mechanism: Favors the EU, not France, Applies to supplies only, not cloud/AI/SaaS or consulting, Applies only to specific contracting entities. France uses regulatory security frameworks, not procurement preferences, to steer certain technology choices: SecNumCloud (ANSSI) for "trusted cloud"[202] – a security requirement, not a buy-local rule, though it effectively favors EU-controlled providers; 5G equipment vetting ("Loi Huawei", 2019)[203] – national-security authorization, not a procurement preference[204]; Defence procurement exemptions (Directive 2009/81/EC + Art. 346 TFEU) – exception-based and unrelated to local preference. This directive creates a lighter procurement framework for defence and sensitive security areas. It permits: limited tendering, negotiated procedures without publication, security-of-supply requirements, security-of-information requirements. These measures influence technology selection but do not constitute "buy local" procurement rules.
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose restrictions on origin of the funds and the manner in which they are invested?	Yes Tax incentives and fiscal exemptions Examples: - Research Tax Credit - Innovation Tax Credit - Young Innovative	France has implemented a broad set of fiscal incentives and public support mechanisms to promote the development of "sovereign" technologies, in particular cloud services, AI, cybersecurity, and microelectronics. These schemes are designed to foster R&D, innovation, and industrial capacity in these strategic domains, while ensuring that public funding remains fully compliant with EU State aid rules.

[202] https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud
[203] https://www.legifrance.gouv.fr/codes/id/LEGIARTI000038867923/2019-08-03
[204]

	Company scheme - “IP-Box” - Energy-efficient data centers No serious conditionality to these incentives	Tax incentives[205] and fiscal exemptions targeted at technological innovation, such as: Research Tax Credit: 30% of qualifying R&D expenditure up to €100 million, then 5% beyond that threshold (mainland France); Innovation Tax Credit: reserved for small and medium compagnies, covering 20% of eligible innovation-related expenditure (mainland France); Young Innovative Company scheme[206] : applicable to firms established before 31 December 2023, granting a full exemption from corporate income tax for the first profitable year, and a 50% exemption for the following profitable year. Additional sector-specific tax mechanisms also exist, including tax reductions for energy-efficient data centers and a dedicated “IP Box” regime under which qualifying intellectual property income is taxed at a reduced 10% rate (instead of 25%), provided that the corresponding R&D activities are performed. Conditionality remains very limited today. Although these tax incentives are subject to a number of eligibility requirements, issues such as long-term localization, job retention, or protection against offshoring cannot be invoked to recover these subsidies or tax advantages. In France, there is indeed an ongoing debate about strengthening the conditionality of public support. At this stage, however, this remains primarily a political and doctrinal discussion rather than a systematic legal framework.
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?	Yes	Cloud Act & U.S. Extraterritorial Access to Data The U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data Act) has been a major concern for France:[207] under its framework, U.S. authorities can compel data disclosure from cloud providers even when data is stored outside the U.S. The French Parliament (via a report) explicitly criticized this, noting the threat it poses to French (and EU) digital sovereignty. [208]

205 https://www.economie.gouv.fr/entreprises/developper-son-entreprise/innover-et-numeriser-son-entreprise/innovation-quels-sont-les

206 https://entreprendre.service-public.gouv.fr/vosdroits/F31188

207 https://questions.assemblee-nationale.fr/q15/15-9260QE.htm

208 https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

		In reaction, France has supported and developed GAIA-X[209], a Europe-led cloud infrastructure initiative, and promoted SecNumCloud, an ANSSI certification regime to limit foreign (especially U.S.) legal reach over European data. *Implication*: U.S. legal reach (via CLOUD Act) is seen as a form of legislative pressure or interference on European data sovereignty — France treats this as a strategic risk in its innovation and data policy. Lobbying by Big Tech (U.S.) on EU Digital / AI Regulations According to the European Parliament, major U.S. tech firms (Google, Microsoft, Amazon, Facebook) are very active in lobbying EU institutions on data protection, digital regulation, and innovation policy.[210] France has played a role in diluting certain AI regulation proposals at the EU level: for example, in AI legislation, France pushed exemptions for law enforcement / surveillance uses. Big Tech (mainly U.S.-based) is seen as influencing EU (and French) digital regulation in ways that may favor their business model, potentially undermining Europe's digital sovereignty. Dependence on Non-European Cloud Providers (Industrial Policy Risk) In the context of the French Health Data Hub, there was strong public debate when Microsoft's Azure[211] was considered for hosting highly sensitive health data. Some French and EU voices raised concerns that entrusting such data to a U.S. provider undermines sovereignty, because U.S. law (e.g., CLOUD Act) could apply[212]. This is not a formal "foreign lawmaking interference" in a legislative text, but it reflects policy influence (economic, technological) that shapes French innovation infrastructure decisions. Significance & Interpretation (from EU / French Legal-Political Lens)

209 https://presse.economie.gouv.fr/gaia-x-lecosysteme-numerique-et-industriel-francais-reuni-a-bercy-accelere-sur-la-creation-despaces-de-donnees-de-confiance/

210 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)751434

211 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000049057224

212 https://www.legifrance.gouv.fr/ceta/id/CETATEXT000049327718#:~:text=Il%20appartient%20au%20juge%20des,de%20la%20d%C3%A9cision%20soit%20suspendue.

		Strategic sovereignty concern: These examples are widely framed in France as part of a *digital sovereignty* struggle. Foreign influence (especially U.S.) over cloud/data infrastructure is seen not just as a commercial risk, but as a threat to legislative autonomy. Regulatory push-back: France's support for GAIA-X and SecNumCloud shows an active attempt to counterbalance U.S. influence with European alternatives. Lobbying risk: The influence of U.S. big tech on EU lawmaking (AI, data) is interpreted by many in France as foreign economic actors shaping the regulatory environment to their advantage — raising concerns about whether regulatory outcomes truly reflect European public interest. Institutional response: More broadly, France (and other EU states) are increasingly attentive to such influence in policy debates, especially given the intersection of data regulation, national security, and economic competitiveness.
Ongoing / Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?	Not seriously	Bill on the *Resilience of Critical Infrastructures and the Strengthening of Cybersecurity*[213] transmitted to the National Assembly: among other provisions, it aims to reinforce national frameworks for the protection of critical activities and to enhance resilience against cyber threats. National implementation of the AI Act regime (designation of competent authorities). Data Act (EU Regulation 2023/2854): obligation for France to establish and notify a national sanctions and enforcement regime (EU deadline: 12 September 2025). Implementing decrees of the Law on Securing and Regulating the Digital Space (SREN) of 21 May 2024.

[213] https://www.senat.fr/dossier-legislatif/pjl24-033.html

Germany

Alexander Tribess, GreenGate Partners Rechtsanwaltsgesellschaft GmbH, Hamburg
Dr. Philip Kempermann, Heuking, Dusseldorf

Executive summary

Germany approaches technological autonomy as a strategic priority that is deeply embedded across its digital, industrial, and innovation policies. Rather than relying on a single framework, Germany pursues technological sovereignty through a series of interlocking national strategies, including the Digital Strategy 2030, multiple cloud and data initiatives, a comprehensive AI strategy, and strong commitments to European cooperation. The country positions technological autonomy as both an economic imperative and a matter of national and European security.

The private sector as well as the government to a large extent makes use of hyperscalers for their technology applications. This creates dependencies on service providers that are under the jurisdiction of non-EU countries. Therefore, a central driver of Germany's approach is the desire to reduce structural dependencies on non-EU cloud and technology providers. This concern informs the Federal Multi-Cloud Strategy, the development of the Deutsche Verwaltungscloud (DVC) for public administration, and Germany's prominent role in GAIA-X and the broader European data and cloud ecosystem. These initiatives are complemented by Germany's open-source strategy, which explicitly promotes open technologies as a means to strengthen sovereignty, security, and interoperability. The political salience of technological autonomy has intensified in recent years, with the federal government openly advocating for European digital sovereignty and embedding this objective in sector-specific policies such as the National Security and Defence Industry Strategy.

Germany's National AI Strategy forms another major pillar of its autonomy agenda. The country has invested heavily in AI research infrastructure, creating six national centres of excellence and supporting the emergence of domestic foundational models such as Aleph Alpha and OpenGPT-X. These efforts are supported by the AI Action Plan 2023 and significant public funding aimed at building an advanced, sovereign AI ecosystem capable of meeting industrial and public-sector needs. In parallel, Germany continues to expand its high-performance computing landscape and its quantum computing capabilities, as seen in major national initiatives such as the DLR Quantum Computing Initiative, the Fraunhofer Quantum Systems Programme, and the Munich Quantum Valley. Collectively, these programmes aim to create domestic capability in cutting-edge compute hardware, algorithms, and applications that underpin long-term autonomy.

Despite these advances, there are several threats to technological autonomy. Germany remains concerned about over-reliance on foreign hyperscalers and exposure to non-EU lawful-access regimes, which reinforces the push for sovereign cloud solutions. Other perceived threats include the global concentration of market power among dominant digital platforms and broader geopolitical dependencies in critical technologies such as semiconductors and telecommunications equipment. These concerns are reflected in Germany's enforcement of competition rules (notably §19a of the German Competition Act) and in the integration of sovereignty objectives into cybersecurity policy under KRITIS and the forthcoming NIS2-based regulatory framework.

At the same time, Germany can point to noteworthy success stories. The most recent big success story is DeepL, the automated translated powerhouse that has changed document

translations worldwide and is still independently owned and based in Germany. The launch of the Deutsche Verwaltungscloud in 2025 marks an important milestone for sovereign public-sector IT infrastructure. The country's growing portfolio of quantum computing platforms, such as Quantum System One and QVLS-Q1, demonstrates a commitment to domestic hardware and ecosystem development. Additionally, Germany's leadership in European cloud, data, and AI initiatives positions it as a central architect of Europe's collective technological sovereignty.

Across these developments, several sectors stand out as focal points for implementing technological autonomy policies, including public administration, defence, critical infrastructure, and high-value industrial domains such as automotive, manufacturing, and chemicals. The technologies most closely associated with Germany's autonomy agenda are artificial intelligence, cloud and sovereign data infrastructure, quantum computing, cybersecurity, and open-source software.

Defining Technological Sovereignty	
How is technological sovereignty defined in your jurisdiction? What are the most important factors considered? Examples of Factors: ● Political ● Social ● Dependency perspective ● IT Infrastructure ● Legislative perspective (various levels)	Digital sovereignty is generally defined by German government agencies as *"the ability and possibility of individuals, companies, and state institutions to act independently, self-determinedly, and securely in the digital space"*.[214] This concept focuses not on isolation, but on ensuring that Germany and Europe retain the capacity to make autonomous technological decisions. The German Federal Government first articulated its comprehensive Digital Strategy in 2020.[215] Building on this framework — and accelerated by geopolitical developments such as the COVID-19 pandemic, the Russian invasion of Ukraine, rising trade restrictions, and global supply chain vulnerabilities — the government has identified strengthening digital sovereignty as a strategic priority. A key pillar is the development of a trustworthy European cloud infrastructure, based on open interfaces, interoperable European standards, and the increased use of open-source technologies. Germany consistently emphasizes that digital sovereignty cannot be achieved through national measures alone. Instead, it requires coordinated European action, particularly in areas such as artificial intelligence, secure cloud infrastructures, zero-trust architectures, and open-source ecosystems.[216] Reflecting this, the governments of Germany and France convened a Summit on European Digital Sovereignty on 18 November 2025, inviting EU Member States to collaborate on joint initiatives aimed at

[214] Digitale Souveränität, Kompetenzzentrum Öffentliche Informationstechnologie (ed. Gabriele Goldacker), 2017, https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet/Digitale%20Souver%c3%a4nit%c3%a4t.pdf.

[215] https://www.bmv.de/DE/Themen/Digitales/Digitalpolitische-Strategien-und-Schwerpunkte/Digitalstrategie-der-Bundesregierung/digitalstrategie-der-bundesregierung.html.

[216] Website of the Federal Commissioner for Information Technology: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html#doc18094248bodyText1.

	strengthening Europe's technological resilience, security, and innovation capacity.[217]	
Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?	No	Germany has not issued a single dedicated cloud sovereignty policy document. However, it has embedded cloud sovereignty goals into broader digital strategies and launched several initiatives to bolster sovereign cloud capabilities. The Federal IT Planning Council adopted a German Administrative Cloud Strategy (Deutsche Verwaltungscloud-Strategie, DVS) as part of a program to strengthen the digital sovereignty of public IT. ⇨ Strategy seeks to build a secure, sovereign multi-cloud infrastructure for government Major policy steps and projects include: **Federal Multi-Cloud Strategy:** The government's multi-cloud approach lets public agencies use a mix of providers under strict conditions. This prevents over-reliance on any single foreign vendor and strengthens digital sovereignty by allowing independent choice of technologies. For example, the federal IT service center (ITZBund) has adopted a "cloud-first" policy and in 2024 chose a German cloud (IONOS) to host many federal systems. All external cloud services must meet high security standards to be used for government data. **Government Cloud (DVC):** In March 2025 Germany launched its own government cloud platform, Deutsche Verwaltungscloud (DVC), after 18 months of development. The DVC offers standardized cloud services to agencies nationwide, providing a sovereign environment operated by the government. **European Initiatives:** In 2019 Germany (with France) launched **Gaia-X**, a federation of cloud providers aiming to create a secure, interoperable European data infrastructure. Germany's federal projects also align with EU frameworks like the upcoming EU Cloud Rulebook and "European Alliance for Industrial Data and Cloud," which encourage EU-wide standards for trusted cloud services In May 2025, Germany created a new Federal Ministry for Digital Transformation and Government Modernisation ("Digitalministerium"). The mission is to modernise the state, cut bureaucracy and use digital technologies (especially AI) – to drive growth. AI is a top priority for the work of this new ministry. It's goal is that the state will become an anchor customer for

[217] https://bmds.bund.de/aktuelles/eu-summit.

		digital and AI solutions so that innovative products are not just tested elsewhere but built and scaled in Germany. Germany has an updated data-centre, energy and compute strategy, and is investing in AI factories in research and industry to secure the capacity Europe needs. => Goals: strong European cloud providers (building partnerships to help them grow)
AI and Technology Sovereignty policy		
Has your jurisdiction published a national technology sovereignty policy?	No National Security and Defence Industry Strategy[218]	Germany has a coherent technology-sovereignty strategy, but it is modular rather than distilled in one single law or "National Technology Sovereignty Policy". Key levers are the Deutschland-Stack, sovereign cloud infrastructure, open-source policy, and cross-ministry digital strategy. Key pillars include: ● The federal government's Digital Strategy 2030, which lists "digital sovereignty" as one of its core goals. ● Major federal programs such as GAIA-X (a European cloud and data infrastructure initiative) and Sovereign Cloud Germany, aimed at reducing strategic dependencies on non-EU cloud providers. ● Funding initiatives under the Federal Ministry for Economic Affairs (BMWK) promoting sovereign cloud services, open-source technologies, semiconductor independence, cybersecurity, and secure digital infrastructure. An important sector-specific anchor within this landscape is the National Security and Defence Industry Strategy, which supplements the general digital-policy instruments with defense-focused requirements. It emphasizes the need for German and European sovereignty in critical IT, cybersecurity, and defense-relevant technologies as a prerequisite for safeguarding peace, security, and strategic autonomy. This reflects Germany's broader view that technological sovereignty must be developed both horizontally across government and vertically within sensitive sectors such as defense.

218 https://www.bmvg.de/resource/blob/5873628/138fddf8112609dfdc3ea44a52ba9195/dl-national-security-and-defence-industry-strategy-data.pdf.

Does your jurisdiction have a published national AI strategy/policy?	Yes	Germany has a fully published and regularly updated National AI Strategy, originally adopted in 2018 and expanded in 2020 and 2023. Key elements include: ● Strengthening AI research and infrastructure. ● Ensuring safe, ethically responsible, and human-centric AI development. ● Supporting industrial adoption of AI across manufacturing, chemicals, automotive, and public services. ● Attracting AI talent and improving compute capacity. ● Aligning national policy with the EU AI Act. The strategy is publicly available and forms the cornerstone of Germany's AI governance and innovation policy.
Does your jurisdiction have a published AI compute or cloud strategy/policy?	Yes	Germany has **several** policy frameworks addressing AI compute, cloud infrastructure, and sovereign data ecosystems: **Cloud & Sovereign Infrastructure Strategies** ● **GAIA-X**: a Franco-German initiative defining standards, interoperability rules, and governance for sovereign cloud and data spaces in Europe. ● Sovereign Cloud Germany: promoted by BMWK and BSI to support EU-based hosting for sensitive workloads. **AI Compute Strategy** While not consolidated in a single "AI Compute Strategy" document, Germany's AI policy includes: ● Investments in **high-performance computing (HPC)** centers for AI training and research. ● Funding for **GPU clusters and national compute centers**. ● A roadmap for "AI-ready" cloud and data infrastructure to support research, industry, and public sector AI systems. Germany's cloud and compute strategy is tightly coordinated with broader **EU initiatives** (Data Act, Data Governance Act, AI Act, European AI Factories, Chips Act).

How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks related to technological sovereignty?	n.a.	The political and public debate around digital and technological sovereignty in Germany is very active and highly salient. Key drivers: ● Concerns about reliance on U.S. hyperscalers (AWS, Azure, Google) and potential exposure to U.S. CLOUD Act obligations. ● Awareness of geopolitical dependencies (e.g., Chinese telecom equipment, global semiconductor supply chains). ● Enforcement pressure from GDPR/Schrems II cases, pushing organisations toward EU-based hosting. ● EU-wide initiatives on cloud, data spaces, and secure digital infrastructure. Digital sovereignty is discussed frequently in Germany's parliament, and multiple legislative proposals in 2024–2025 highlighted: ● The need to map and reduce foreign dependencies, ● Strengthening national and EU tech capabilities, ● Aligning national policy with the EU AI Act and the forthcoming Cyber Resilience Act. It is a structural political theme, not a temporary trend.
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	Yes	AI Foundation Model Development in Germany: Aleph Alpha GmbH (private sector) = German startup based in Heidelberg (founded 2019) that develops large language models (LLMs) and AI solutions for enterprise and government. OpenGPT-X with "Teuken-7B" = The OpenGPT-X project is a German-led consortium (including Fraunhofer Gesellschaft, TU Dresden, and others) funded by Germany's Federal Ministry for Economic Affairs (BMWK) to develop an open multilingual large language model "Made in Germany". LeoLM (by LAION & Hessian.AI) = is a series of open-source, commercially usable large language models optimized specifically for the German language.

Does your jurisdiction have national AI research centres of excellence?	Yes[219]	Network of German Centres of Excellence for AI Research The Network of German Centres of Excellence for AI Research is comprised of six leading research institutions in the field of Artificial Intelligence: BIFOLD, DFKI, MCML, LAMARR, ScaDS.AI Dresden/Leipzig and TUE.AI Center. Together, they work towards strengthening Germany as a top-tier location for AI technologies as well as increasing the national and international visibility of German AI research. The synergies created in the collaboration of the National Centres of Excellence for AI Research are based on intensive exchange of competencies and research results as well as the implementation of joint activities. The Network of German Centres of Excellence for AI Research is formed by the cooperation of the recognized competence centers ⇨ BIFOLD, represented by Technische Universität Berlin, ⇨ DFKI, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH ⇨ MCML, represented by Ludwig-Maximilians-Universität München ⇨ LAMARR, represented by Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. ⇨ SCADS.AI, represented by Technische Universität Dresden ⇨ TUE.AI, represented by Eberhard Karls Universität Tübingen The cooperation does not establish a corporate relationship or partnership between the network partner under corporate law. In particular, the partners have expressly excluded the formation of a civil law partnership.
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes	1. Research & public infrastructure Germany has multiple, well-funded hubs that build and operate quantum computers Fraunhofer & IBM – Quantum System One (Ehningen) Fraunhofer and IBM installed Europe's first IBM Quantum System One in Ehningen, Baden-Württemberg. It's a 27-qubit machine operated

219 https://www.dfki.de/en/web/qualifications-networks/networks-initiatives/centres-of-excellence-for-ai-research

		in Germany and used as a research and industry platform via Fraunhofer's quantum computing network. Munich Quantum Valley (Bavaria) MQV is a Bavarian initiative (LMU, TUM, Max Planck Institutes, etc.) whose explicit mission is to develop and operate competitive quantum computers in Bavaria and transfer that knowledge to industry. Quantum Valley Lower Saxony (QVLS) QVLS is building the QVLS-Q1 ion-trap quantum computer: a 50-qubit system intended to be completed by 2025, explicitly branded as a "quantum computer made in Lower Saxony". DLR Quantum Computing Initiative (DLR QCI) The German Aerospace Center (DLR) runs the DLR QCI with innovation centres in Ulm and Hamburg. It covers the full stack: hardware, software, applications, manufacturing tech and supply chains, and provides labs/cleanrooms to industrial partners. On top of that, there are long-standing quantum research clusters (e.g. QUEST in Hannover, MPQ in Garching, etc.) that feed talent and technology into these initiatives. **2. Domestic development of quantum hardware** Germany is designing and building its own quantum computers on several platforms: **Ion-trap systems:** QVLS-Q1 (Lower Saxony): 50-qubit ion-trap machine under development DLR QCI has multiple ion-trap hardware projects and has awarded contracts for ion-based systems to German companies. **Neutral-atom systems:** planqc (Garching, spin-off of Max Planck Institute for Quantum Optics) builds neutral-atom quantum computers **Trapped-ion manufacturer:** QUDORA Technologies (Braunschweig) is a German manufacturer of trapped-ion quantum computers and is now preparing to present its upcoming system at its German HQ. **LR QCI multi-technology program:** DLR QCI reports 17 hardware projects across five qubit technologies and is explicitly meant to build German quantum computers and a domestic supply chain. **3. Commercialization** DLR Quantum Computing Initiative (QCI) Planqc

		eleQtron QUDORA
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	No	Under German (and EU) law there is no general property right in data as such.
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?	Yes	Within German jurisdiction there is a special statutory regime for text and data mining (TDM), because Germany implemented the EU DSM Directive (2019/790) into the UrhG. These provisions explicitly create TDM exceptions beyond general copyright limitations. Germany implemented two separate TDM exceptions in §§ 44b and 60d UrhG. § 44b UrhG: General text and data mining (for any purpose) § 60d UrhG: TDM for scientific research
Does your jurisdiction have (1) an open, principle-based notion of "fair use" or (2) a closed, listed exceptions-based notion of "fair dealing"? Do those rules favor national players?	Yes	Germany's regime is based on closed listed exceptions. Even though Germany has no general "data ownership" right, these TDM exceptions function as a pro-innovation regime, because they: ● Protect AI developers when making training copies ● Reduce transaction costs for machine-readable content access ● Explicitly allow commercial TDM in § 44b ● Guarantee research freedom through § 60d
Have courts in your jurisdiction issued decisions on the application of "fair dealing" or "fair use" in relation to the use of unlicensed data to train AI models (i.e. via screen scraping)?	No	No, the German courts can not apply fair use. That said, German courts have already decided cases about using unlicensed, scraped data to train AI models. They analyse it under the statutory copyright exceptions, especially the text and data mining (TDM) rules (§§ 44b, 60d UrhG), not under a "fair use" label. In a recent decision (LG München I, 42 O 14139/24), the court found in GEMA v. OpenAI that the memorisation and output of protected song lyrics constituted copyright infringements not exempted by the TDM rules. This decision is highly debated in the German legal scene and will be reviewed under appeal. The debate will very likely not be finally settled for another few years.

Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?	No	No, there are not. To the contrary, the EU Data Act breaks up any factual exclusivity, at least when it comes to non-personal connected device data.
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: c) in the public sector? d) in the private sector?	a) No b) No	**a) Public sector** Germany does **not** have a general statutory data-localization requirement for public authorities. However, several sector-specific rules create **functional localization obligations**: ● **Classified government information** (VS-NfD / VS-VERTRAULICH / GEHEIM / STRENG GEHEIM) must be processed **only on infrastructure located in Germany or within certified secure EU environments** (based on the *Verschlusssachenanweisung – VSA*). ● Public-sector IT security guidelines issued by the **Federal Office for Information Security (BSI)** strongly recommend the use of **"sovereign cloud"** or EU-based environments, particularly for ministries, police, defence, and national security sectors. ● Certain **health, police, and tax information systems** must operate within Germany or the EU due to sector legislation (e.g., SGB, police laws of the Länder, fiscal secrecy rules). These rules do not constitute a general "data localization law," but they **function as localization** for categories of sensitive public-sector data. **b) Private sector** Germany has **no localization requirements** for private-sector data. Under the GDPR, private organizations may store and process data anywhere in the world **provided all GDPR Chapter V safeguards are met**: ● Adequacy decision (Art. 45) ● Standard Contractual Clauses (Art. 46) ● Binding Corporate Rules (Art. 47)

		• Derogations in exceptional cases (Art. 49) No additional German rules impose stricter cross-border restrictions for companies.
What are special classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?		Germany classifies certain public-sector information as **VS-NUR FÜR DEN DIENSTGEBRAUCH**, **VS-VERTRAULICH**, **GEHEIM**, and **STRENG GEHEIM** under the **German Federal Security Classification Rules (VSA)**. Such data must be **hosted and processed only within Germany (or approved secure facilities)**. Legal basis: **VSA**, intelligence-security laws, and internal security regulations of federal and state ministries. → These rules **do not apply to private-sector personal data**.
What are the most notable cross-border data transfer restrictions in your jurisdiction?		Germany applies **GDPR Chapter V**: • Transfers allowed only with an **adequacy decision**, or • **SCCs**, **BCRs**, Art. 49 derogations, and • **Transfer impact assessments (TIAs)** post-Schrems II. **A**dditional German-specific restrictions, e.g. for social security data pursuant to SGB X.
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?		**ECJ, Schrems II (C-311/18)** – invalidated EU-US Privacy Shield; mandated TIAs; strong obligations for exporters. **German DPAs (e.g., Baden-Württemberg, Berlin)** – enforcement actions requiring companies to suspend US transfers where TIAs could not mitigate US surveillance risks.
Information Security Laws for Critical Infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Yes	Germany has a well-developed information-security (cybersecurity) regime for critical infrastructure (KRITIS), that is covering both state-owned and private-sector operators. These rules require special legal, technical, and organizational considerations. Under the Core Legal Framework: BSI-Gesetz (BSIG) + KRITIS Regulation, companies must (a) Implement "state-of-the-art" IT-security (§ 8a BSIG) (b) Have security management systems (c) Mandatory audits every 2 years (d) Mandatory incident reporting

		(e) Appointment of a KRITIS contact/ liaison NIS2 Transformation: The KRITIS-Dachgesetz (KRITIS-DachG) Germany is implementing the EU's NIS2 Directive through the new KRITIS-Dachgesetz, which will significantly broaden the number of regulated entities and tighten security obligations. NIS2 introduces board-level responsibility, stricter risk- and supply-chain management requirements, and a three-stage incident-reporting regime (24h/72h/one month). Fines and supervisory powers increase substantially, meaning that many organisations will need to upgrade their governance, vendor oversight, and documentation practices.
In your jurisdiction, can directors and officers be held accountable for not diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?	Yes	Yes, directors and officers in Germany can be held accountable. There is not a specific statutory duty to "diversify suppliers", but because German corporate, regulatory, and sector-specific laws impose broad management duties that include mitigating concentration risks in critical digital infrastructure. However, multiple intertwined legal norms functionally impose such a duty whenever concentration creates material operational, security, or compliance risk. i.E.: § 93 AktG / § 43 GmbHG – Duty of care and business judgment
Lawful Access (Legal Access to Data without Consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit	Yes/	Several statutes grant German authorities access to data held by telecoms, cloud providers, and enterprises: ● Telecommunications Act (TKG) – metadata disclosure; real-time interception. ● Code of Criminal Procedure (StPO) – seizures, production orders, access to cloud data. ● Police laws of the Länder – preventive access. Foreign authorities cannot directly access data; access must occur via Mutual Legal Assistance Treaties or EU judicial cooperation mechanisms.

lawful access by foreign authorities?		
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a "collect all" regime) under such lawful access regime?	No	Access must relate to specific persons, identifiers, or events. Bulk collection is constitutionally limited by German Constitutional Court (BVerfG) jurisprudence on proportionality and informational self-determination.
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?	No	For criminal investigations: judicial authorization generally required (StPO). For intelligence services: some forms of strategic surveillance allowed under the G10 Act, subject to G10 Commission oversight (quasi-judicial). Police preventive powers differ by state; warrantless access possible but under strict statutory conditions.
Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Yes	• EU–US MLAT, • Budapest Convention on Cybercrime, • Prüm Decisions, • EU–UK Trade and Cooperation Agreement (law enforcement cooperation). None of these agreements allow foreign authorities direct access to data in Germany, but they may facilitate cross-border lawful access requests.
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation? What is their most notable impact on promoting technological autonomy?	n.a.	The most important statutory regime in Germany intended to promote competitive markets for innovation is the German Competition Act (GWB), especially § 19a GWB. Its most notable impact is enhancing Germany's and Europe's technological autonomy by limiting Big Tech gatekeeper power, enforcing interoperability, and preventing market foreclosure. This enables the domestic and European innovation systems to grow. Because it directly targets the market power and gatekeeping behaviour of dominant digital and technology players.

		Competition law does not promote innovation by subsidy, but by preventing market foreclosure, which is the precondition for innovation by newcomers. The Digital Markets Act (DMA) complements § 19a GWB by imposing uniform EU-wide obligations on gatekeepers. Both regimes operate in parallel: § 19a enables swift national intervention, while the DMA provides a harmonised framework. Together, they reinforce competitive conditions and support technological autonomy.
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?	Yes	The German competition regime, especially § 19a GWB, has been actively applied by the Bundeskartellamt and confirmed by courts. These applications advance innovation by curbing dominant gatekeepers and thus support the broader goal of technological autonomy (by enabling alternative players and reducing dependency). Proceeding against Google based on new rules for large digital players (Section 19a GWB) – Bundeskartellamt examines Google's significance for competition across markets and its data processing terms[220] Bundeskartellamt gives users of Google services better control over their data *Alphabet Inc., Google's parent company, gives users better choice as to how Google processes their data according to Commitments undertaken by Google. The Commitments are the result of a proceeding conducted by the Bundeskartellamt based on the new instrument under competition law, which allows the Bundeskartellamt to intervene when competition is threatened by large digital companies (Section 19a of the German Competition Act, GWB). The new provision was introduced in 2021. The proceeding is a testament to the close cooperation between the Bundeskartellamt and the European Commission on the way to achieving more competition and fair markets in the digital sector.* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/05_10_2023_Google_Data.html

220 https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/25_05_2021_Google_19a.html

		The Bundesgerichtshof (BGH: Germany's Federal Court of Justice) confirmed in May 2024 that the Bundeskartellamt rightly designated Amazon.com, Inc. as an undertaking of paramount cross-market significance under § 19a(1) GWB.[221] These decisions have several implications relevant to technological autonomy: By designating large digital platforms and intervening in their practices (e.g., combinations of data across services, restricting interoperability), the Bundeskartellamt is reducing structural barriers to competition in digital markets. For startups, alternative cloud/AI providers, European or German tech firms, this creates more space to enter markets previously locked by dominant ecosystems. For technological autonomy (in the sense of reducing dependency on a few global tech giants), the decisions matter because they force dominant firms to open up or modify their business models (e.g., Google's commitments to data access). This helps domestic/European firms access necessary infrastructure, data, or platforms. The alignment of § 19a GWB enforcement with the Digital Markets Act (DMA) (EU-level gatekeeper regulation) means Germany is using its competition law regime to anticipate and underpin a regulatory framework supportive of digital sovereignty.
Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes") ?	Yes	Germany is bound by EU trade agreements. Notable examples: ● CETA, EU–Japan EPA, EU–Korea FTA – include provisions on digital trade and government procurement Germany is not part of the US CLOUD Act regime or "Five Eyes." However, the US CLOUD Act may affect US providers operating in Germany, which is relevant indirectly.
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	No	Germany does not have explicit "buy local" rules for tech procurement at federal level. Procurement is governed by EU procurement law (non-discrimination, open competition). Some public tenders include sovereignty/security preferences, but not formal "local content" requirements.

[221] https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/FR/2024/2024097.html

Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose restrictions on origin of the funds and the manner in which they are invested?	No	Germany does not have a single "Technological Autonomy Incentive Act," but it has a cluster of tax incentives, subsidies, and public-funding programs. Germany provides tax and financial incentives supporting technological autonomy mainly through: ● the R&D Tax Credit (FZulG) ● IPCEI projects in chips, cloud, quantum, and energy ● BMBF/BMWK digital sovereignty programs These incentives do not impose nationality restrictions. But they do impose: ● location-of-R&D requirements (work must be done in Germany/EU) ● state aid compliance ● and in some programs, security constraints relating to data location, vendor trustworthiness, or extraterritorial control These instruments promote technological autonomy indirectly by building domestic capabilities. *The Act on Tax Incentives for Research and Development (Forschungszulagengesetz – FZulG) of December 14, 2019 introduced a new tax incentive for research and development in the form of a research allowance. The tax incentive complements the well-developed project funding landscape and is intended to strengthen Germany as an investment location and stimulate research activities, particularly among small and medium-sized enterprises.* *IPCEI (Important Projects of Common European Interest)* *The EU's 'Important Projects of Common European Interest' (IPCEI) scheme is one of the bloc's key instruments for transforming its economy in the name of climate neutrality. The EU's two largest economies,* ***Germany*** *and France, are among the states most eager to enter into multinational partnerships and revive or kickstart sustainable industries by making use of eased state aid rules and strategic cooperation for future technologies. Despite significant differences in other energy and climate policies, Paris and Berlin hope that the IPCEI will serve to boost the domestic production of batteries, hydrogen, and renewable power installations as a platform for their future competitiveness.*

		Funding programs: *KMU-innovativ* *Bundesagentur für Sprunginnovationen (SPRIND)* *= Revolutionäre Ideen haben eine Chance verdient. Die Bundesagentur für Sprunginnovationen (SPRIND) ermöglicht die Förderung von Innovationen, die das Potenzial haben, die Welt positiv zu beeinflussen.* *BMBF AI Strategy funding* *= The BMFTR provided five million euros in funding over five years for researchers doing experimental work in AI research.* *BMWK Digital Sovereignty & Gaia-X funding lines*
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?	Yes	Direct “interference” is rare. However: ● US surveillance laws (FISA 702; CLOUD Act) have strongly influenced German/EU data-transfer laws and cloud-sovereignty policy. ● Schrems/NOYB litigation (Austria-based but globally significant) has shaped German data-protection enforcement. ● International pressure and interoperability concerns influenced Germany’s implementation of the EU Data Act, EU Data Governance Act, and AI Act.
Ongoing / Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?	Yes	Germany’s jurisdiction is currently in the process of a material law reform that is likely to have a significant impact on issues related to technological autonomy. The key legislative initiative is the KRITIS-Dachgesetz. It will strengthen the resilience and security requirements for critical digital and physical infrastructure, thereby reducing dependencies on single suppliers and enhancing Germany’s ability to operate essential systems independently. Further, the foundation of the new Digitalministerium will likely lead to further initiatives.

Italy

Licia Garotti, Pedersoli Gattai, Milan
Marco Galli, Pedersoli Gattai, Milan

<table>
<tr><th colspan="2">Executive summary</th></tr>
<tr><td colspan="2">Italy's technological autonomy strategy is strongly aligned with the European Union's broader vision of digital and strategic sovereignty. The country prioritizes reducing dependence on non-EU technology providers, ensuring greater control over critical data, and strengthening resilience in key digital infrastructures. Italy, alongside its national initiatives, embeds its policies within EU regulatory frameworks, which collectively shape the country's approach to data governance, cybersecurity, and safe AI development.

Technological sovereignty is pursued primarily through coordinated European programs, complemented by targeted national measures. Domestically, Italy is enhancing its capabilities in high-performance computing, AI research, and space governance. The national innovation ecosystem is supported by research centers of excellence, expanding compute infrastructure, and tax incentives designed to stimulate R&D and technological innovation.

Regulatory and competition authorities play an increasing role in safeguarding technological independence by scrutinizing data practices, limiting lock-in risks, and ensuring contestable digital markets. Additionally, while Italy has no explicit "buy local" requirements, national security tools help protect strategic sectors from excessive foreign influence.

Overall, Italy is evolving toward a more sovereign and resilient technological framework. Its progress is marked by significant investment in strategic infrastructures, growing attention to data governance and digital risk, and alignment with EU policies that collectively drive the country's long-term goal of reinforcing its technological and industrial autonomy.</td></tr>
<tr><th colspan="2">Defining Technological Sovereignty</th></tr>
<tr><td>How is technological sovereignty defined in your jurisdiction? What are the most important factors considered?
Examples of Factors:
● Political
● Social
● Dependency perspective
● IT Infrastructure
● Legislative perspective (various levels)</td><td>Definition of digital sovereignty by the European Parliament: the European Parliament, in its report dated 11 June 2025[222], emphasized that European Union sovereignty consists of the ability to develop capabilities, resilience and security by reducing strategic dependencies and avoiding reliance on foreign actors and individual service providers, while safeguarding critical technologies and infrastructure. The Parliament stressed the need to strengthen EU industrial policy and enhance internal research, development, and manufacturing capabilities in strategic technologies to ensure the EU's preparedness and resilience. With regard to technological sovereignty specifically, the European Parliament stated that it is <u>the ability to design, develop and enhance the digital technologies necessary for EU economic competitiveness, the well-being of its citizens and the EU's open strategic autonomy in a globalized world</u>. Therefore, it is necessary to ensure that the EU can take autonomous decisions, engage in dialogue with third countries and</td></tr>
</table>

[222] See Report on European technological sovereignty and digital infrastructure https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_IT.html.

	trusted third-country entities, diversify and strengthen supply chains, and promote openness and interoperability, so that EU remains an attractive place to invest. From a regulatory perspective, digital sovereignty is supported by regulations such as the Regulation (EU) 2016/679 ("**GDPR**")[223], the Directive 2002/58/EC ("**e-Privacy Directive**")[224] the Regulation (EU) 2022/868 ("**Data Governance Act**")[225], the Regulation (EU) 2023/2854 ("**Data Act**")[226], and the Regulation (EU) 2024/1689 ("**AI Act**")[227].	
Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?	Yes. The Italian Department for Digital Transformation (*Dipartimento per la trasformazione digitale* - "**Digital Department**"), in collaboration with the National Agency for Cybersecurity ("**ACN**") published the "Italy Cloud Strategy: Strategic guidelines for public administration" ("**Italian Cloud Strategy**")[228]	In 2021, Italy adopted the Italian Cloud Strategy centered on public data sovereignty. The Digital Department introduced the Italian Cloud Strategy, built on three pillars: *(i)* classifying public-sector data and services by sensitivity level; *(ii)* certifying cloud services that meet defined security requirements; and *(iii)* creating a dedicated national cloud infrastructure. To implement the third pillar, the Digital Department promoted the establishment of the National Strategic Hub S.p.A. (*Polo Strategico Nazionale* - "**PSN**")[229], a newly company owned by TIM S.p.A., Leonardo S.p.A., Cassa Depositi e Prestiti S.p.A., and Sogei - Società Generale d'Informatica S.p.A.. The PSN is designed as a highly reliable government cloud environment for hosting the critical and strategic data and services of public administrations. The goal is to migrate at least 75% of Italian public administrations to the cloud by 2026, reducing costs and operational risks. Both the Italian Cloud Strategy and the PSN require that strategic and critical data is stored on infrastructure capable of eliminating risks associated with non-EU jurisdictions. Cloud providers must comply with EU data-localization rules and adopt measures that neutralize the extraterritorial effect of foreign laws (such as the U.S.

[223] See full text of the regulation https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[224] See full text of the directive https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng.
[225] See full text of the regulation https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng.
[226] See full text of the regulation https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.
[227] See full text of the regulation https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[228] See official website of the policy https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/ (last updated 19 May 2025).
[229] See official PSN's website https://cloud.italia.it/strategia-cloud-pa/polo-strategico-nazionale

		Cloud Act). In essence, Italy favors a sovereign-cloud approach (also in cooperation with European partners) to ensure that sensitive data remains under national and EU legal control. This is aligned with EU initiatives such as Gaia-X[230], to which Italy actively contributes through its national hub, aimed at building an EU-associated cloud ecosystem with shared standards for interoperability, security, and regulatory compliance. While Italy maintains a "cloud-first" policy open to commercial providers, these measures reduce exclusive reliance on foreign hyperscalers and strengthen contractual requirements related to data sovereignty and business continuity.
AI and Technology Sovereignty Policy		
Has your jurisdiction published a national technology sovereignty policy?	Partially Italy participates in EU strategies aimed at developing safe and high-performance connectivity infrastructures. However, there is not yet a general national technology sovereignty policy. Only in the space sector, even if only indirectly, Italy has enacted a national legislation to promote technological sovereignty.	In the field of networks and digital infrastructure, Italy plays an active role in EU strategies aimed at developing secure and high-performance connectivity systems (5G/6G, fiber optics, satellite networks). The National Recovery and Resilience Plan ("**PNRR**") allocates substantial funding (around Euro 6.7 billion) to ultra-broadband and 5G deployment, with the goal of covering grey and rural areas and meeting the targets of the "Gigabit Society". To safeguard sovereignty and security, the government has exercised its special powers (golden power) over the rollout of 5G networks, imposing strict conditions or vetoes on the use of Huawei and ZTE equipment in the most sensitive portions of mobile networks. At the same time, Italy is engaged in EU initiatives such as: - the European Quantum Communication Infrastructure ("**EuroQCI**"), promoted by the European Commission[231], aimed at building secure quantum communication networks; and

[230] See official website of the project https://gaia-x.eu/

[231] See the European Commission website page dedicated to the project https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

		- the BlueMed project and Open Transit cables, consisting of the development of a strategic submarine cable linking Europe and Asia via the Mediterranean, supported by Italian companies, to diversify global internet routes and reduce dependence on the major Atlantic and Asian chokepoints[232]. It is worth mentioning the main policies and regulations in the field of space law and defense (one of the fundamental elements of space policy). Within the defense sector, the concept of strategic and technological autonomy has expanded beyond its original scope. The aerospace sector is repeatedly mentioned among critical infrastructures and technologies for Member States, and components of the EU space programs are listed among the "programs of Union interest" under Article 8 of the Regulation (EU) 2019/452. The return of conflict in Europe has highlighted the strategic relevance of space and digital infrastructures, prompting the Union to reinforce its coordination in the space sector to strengthen security and defense. International instability has acted as a catalyst, prompting the Union to review and modernize its space policy. The national government's 2025 space and aerospace guidelines outline four strategic priorities[233]: *(i)* promoting scientific and technological research; *(ii)* enhancing the competitiveness of national industries; *(iii)* establishing an effective regulatory framework; and *(iv)* identifying priority areas for international collaboration. A key aspect is the government's commitment to technological sovereignty in the space

[232] On 29 October 2025 Telecom Italia Sparkle S.p.A. (the first international service provider in Italy and among the top global operators) and the Cyprus Telecommunications Authority ("**CYTA**", the leading provider of integrated electronic communications in Cyprus) announced the arrival of the BlueMed submarine cable in Cyprus, at CYTA's Yeroskipos landing station; see Sparkle S.p.A. press release https://www.tisparkle.com/media/press-release/sparkle-bluemed-submarine-cable-lands-cyprus.

[233] Italian Government, "*Government guidelines on space and aerospace"*, January 2025, GovernmentGuidelinesOnSpaceAndAerospace

		sector, increasing strategic autonomy while contributing to international technological leadership. To achieve this, Italy plans a multi-year strategy to strengthen competitiveness by 2030 in key sectors such as research, Earth observation, access to space, telecommunications, navigation, Space Situation Awareness, and space exploration (human and robotic), including orbital operations. The guidelines also emphasize national defense and security, aiming to integrate space sector development with strategic priorities. The first step in this direction was taken in June 2025, when the Italian government promulgated its first set of space regulations ("**Law 89/2025**")[234]. Law 89/2025 indirectly establishes the state autonomy through various provisions (*e.g.,* the obligation for space operators to obtain authorization, which can only be obtained following approval by the Italian authorities, the establishment of the Italian Space Agency - "**ASI**" as the supervisory authority, the provision of administrative and criminal penalties, the provision of a national register for the registration of space objects, and the provision of insurance coverage for authorized operators).
Does your jurisdiction have a published national AI strategy/policy?	Yes The Italian Digital Agency ("**AgID**") published the Italian Artificial Intelligence Strategy 2024-2026 ("**Italian AI Strategy**")[235]	The Italian AI Strategy has been prepared by a committee of experts (to which AgID – the National Digital Authority – provided its technical support) to guide national AI regulation and policy. It outlines strategic priorities in four areas: *(i)* research; *(ii)* public administration; *(iii)* business; and *(iv)* education, emphasizing ethical, safety, and inclusive AI development. The Italian AI Strategy aligns with EU initiatives and Italy's role in the G7. Government officials stress the goal of leveraging national strengths and promoting trustworthy AI

[234] Law no. 89 of the 13 June 2025, Gazzetta Ufficiale

[235] See official website of the policy https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2024/07/22/pubblicato-il-documento-completo-strategia-italiana-lintelligenza-artificiale-2024.

		solutions. In addition, Article 19 of Italian Law no. 132/2025 ("**AI Italian Law**")[236] requires the national Italian AI Strategy to be updated every two years by the Digital Department, with oversight from the interministerial committee for the digital transition ("**CITD**") that also coordinates industrial measures and incentives. On the investment side, the PNRR funds major initiatives such as the National AI Center FAIR foundation[237] (Future Artificial Intelligence Research, with about Euro 320 million) and regional innovation ecosystems like the Rome Technopole foundation[238]. In addition, Italy is a founding member of the Global Partnership on AI ("**GPAI**")[239] and collaborates within the G7 and the Organization for Economic Co-operation and Development ("**OECD**") on responsible AI development. Finally, Italian national authorities also maintain a high level of scrutiny over the development and use of AI, as demonstrated, for example, by the decision

[236] See https://www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/sg?utm_source for the full text of the AI Italian Law.
The AI Italian Law sets out the principles governing the research, testing, development, adoption, and application of AI systems and models. In addition, it promotes the correct, transparent, and responsible use of AI in an anthropocentric context, with a view to seizing the opportunities it offers. Finally, it ensures oversight of the economic and social risks and the impact on fundamental rights of AI. The provisions of the AI Italian Law must be interpreted and applied in accordance with the AI Act.
[237] FAIR aims to advance next-generation AI by integrating theoretical, technological, ethical and sustainability perspectives. It adopts a holistic, multidisciplinary approach to rethink AI foundations and assess its societal impact. The goal is to build AI systems that collaborate with humans, adapt to evolving contexts, and operate safely and responsibly. The project follows a Hub & Spoke structure, with the FAIR Foundation as the hub and research partners as the spokes; see official website of the project https://fondazione-fair.it/.
[238] The Rome Technopole Foundation is the reference point for innovation, research, and training in Lazio. Created to establish an integrated ecosystem between universities, research centers, institutions, and businesses, the Rome Technopole Foundation promotes the development of strategic projects in key sectors such as energy transition, digitalization, and health. The key areas that guide the Rome Technopole Foundation's research and development activities, promoting advanced and sustainable solutions for the challenges of the future, are: *(i)* energy transition; *(ii)* digital transition; *(iii)* health and biopharmaceuticals; see official website of the project https://www.rometechnopole.it/.
[239] The GPAI is an integrated partnership that brings together the OECD members and GPAI countries to advance an ambitious agenda for implementing human-centric, safe, secure and trustworthy AI embodied in the principles of the OECD Recommendation on AI; see official website of the partnership https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html#:~:text=The%20Global%20Partnership%20on%20Artificial%20Intelligence%20%28GPAI%29%20is,the%20principles%20of%20the%20OECD%20Recommendation%20on%20AI.

		of the Italian Data Protection Authority, dated 31 March 2023, to impose a temporary suspension of ChatGPT in order to assess its compliance with the applicable regulatory framework[240]. Overall, Italian policies aim to promote AI research and adoption while ensuring risk mitigation, accountability, and high-quality training data.
Does your jurisdiction have a published AI compute or cloud strategy/policy?	No	In Italy, there is not yet a fully comprehensive and formalized strategy dedicated exclusively to AI compute, although the topic is partially addressed within the Italian AI Strategy and the Italian Cloud Strategy. That said, there are numerous initiatives, infrastructures, and investments already underway - from supercomputers to national and European programs - that effectively contribute to building AI computing capacity in the country[241].
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks related to technological sovereignty?	Yes	In Italy, the discussion around digital sovereignty is active and growing, particularly within institutional, industrial, and academic circles. Although not always central in mainstream media, it has become a political priority linked to national security, technological autonomy, and economic competitiveness. The Government and Parliament consistently incorporate it into strategies on cloud, AI, and cybersecurity, while independent authorities, such as the Italian

[240] See the press release of the Italian Data Protection Authority https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847.

[241] The main initiatives are the following: (a) Leonardo Supercomputer (CINECA, Bologna): a pre-exascale system delivering 240 PetaFLOPS, among the world's most powerful, supporting scientific and industrial research in AI, climate, bioinformatics and aerospace https://leonardo-supercomputer.cineca.eu/it/home-it/; (b) HPC District at the Bologna Technopole: a high-density ecosystem of advanced infrastructures, making Bologna a strategic European hub for supercomputing https://www.supercomputing-icsc.it/en/2024/12/05/innovate-the-first-industrial-supercomputer-of-the-european-euro-hpc-infrastructure/; (c) IT4LIA AI Factory (Ministry of University and Research - ACN, 2025): a national platform featuring a supercomputer optimized for generative AI designed to strengthen technological autonomy and provide integrated HPC-cloud-quantum resources for startups, enterprises and public administrations https://www.mur.gov.it/it/news/martedi-10122024/it4lia-ai-factory-sara-italiana-una-delle-prime-piattaforme-strategiche-di; (d) QuIC - Quantum Italy Consortium: not-for-profit industry association dedicated to the growth of the quantum technology sector and making Europe a global market leader https://www.euroquic.org/.

		Data Protection Authority and ACN, address issues related to data protection, critical infrastructures, and technological dependencies. Moreover, businesses and industry associations also debate technological lock-in and relations with major global providers.
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	No	Although Italy does not (yet) host major foundational AI models entirely developed domestically, the country is rapidly expanding its AI compute capabilities through the Leonardo supercomputer, the Bologna HPC district, and the new IT4LIA AI Factory dedicated to generative AI. At the same time, Italy is advancing quantum infrastructures and industrial initiatives such as the Quantum Italy Consortium. Overall, these initiatives are strengthening Italy's technological autonomy and bolstering the competitiveness of its AI ecosystem.
Does your jurisdiction have national AI research centres of excellence?	Yes	Links to AI research centres of excellence: - Italian Technological Institute (*Istituto Italiano di Tecnologia* - IIT): focused on robotics and cognitive AI https://www.iit.it; - the National Interuniversity Consortium for Information Technology ("**CINI**"), which comprises more than 40 Universities, has its own National Laboratory for Artificial Intelligence and Intelligent Systems ("**AIIS-CINI Laboratory**") https://www.consorzio-cini.it/index.php/it/labaiis-home; - National AI Center - FAIR Foundation https://fondazione-fair.it/; - Bruno Kessler Foundation ("**FBK**"): focused on data science, AI ethics an applied AI https://www.fbk.eu/it/; - Turin Politecnico's Digital Revolution House: EU Digital Innovation Hub

		https://www.polito.it/ateneo/comunicazione-e-ufficio-stampa/poliflash/politecnico-fondazione-crt-e-istituto-italiano-di; - Human Technopole: https://htechnopole.it/.
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes	Italy and the European Union both have solid quantum-computing ecosystems, but their scale and maturity differ. Italy has an active research base and is developing its first domestic quantum systems through the ICSC National Centre in Bologna[242], yet it still lacks large quantum-hardware manufacturers of its own. The EU, by contrast, operates multiple quantum testbeds integrated into EuroHPC[243] supercomputers across several Member States and supports a broader industrial landscape, with companies like IQM, Pasqal and Quandela already commercializing quantum hardware. While Italy's commercialization phase is still emerging, the EU pursues a full value-chain approach through major programs like the Quantum Flagship[244] and EuroQCI (European Quantum Communication Infrastructure)[245], aiming for global competitiveness and large-scale industrialization.
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech stack, funding and adoption.	**Please rate each component on a five point scale and circle the best option** (1 = non-existent; 2 = nascent; 3 = existing but insufficient; 4 = solidly in place; 5 = world leading): 1. **AI compute (GPU equipped) data centres** 1 2 3 4 5 2. **Domestically developed AI foundational models** 1 2 3 4 5 3. **Existence of large high-value databases in high-value sectors of economic activity**	

[242] Please refer to note no. 152.
[243] See official website of the project https://www.eurohpc-ju.europa.eu/index_en?utm_source.
[244] See official website of the project https://qt.eu/?utm_source.
[245] Please refer to note no. 142.

	1 2 3 4 5 **4. Availability of funding/financing for commercialization of innovation** 1 2 3 4 5 **5. Rates of AI adoption** 1 2 3 4 5 **6. Domestic quantum computing research, development and commercialization** 1 2 3 4 5 **7. Domestic military defence industry** 1 2 3 4 5	
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	Yes	Italy has implemented Directive 96/9/EC by introducing a *sui generis* database right (Articles 102-bis et seq. of the Italian Law no. 633/1941 - "**Italian Copyright Law**"). This right protects the maker of a database who has made a substantial investment in obtaining, verifying or presenting its contents, granting the ability to prevent the extraction or substantial reuse of those contents. It operates as an exclusive right distinct from and complementary to copyright and is specifically designed to incentivize the creation and maintenance of databases.
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?	Yes	Italy has implemented Directive (EU) 2019/790 by introducing two new exceptions to copyright for TDM (Articles 70- *ter* and 70-*quater*. of the Italian Copyright Law). In particular: - Article 70-*ter* allows reproduction and/or extraction of works for TDM purposes for scientific research by research bodies and cultural heritage protection institutes, provided they have legal access to the works; such exception is not negotiable, therefore, rights-holders cannot prevent it; - Article 70-*quater*, which allows TDM for any purpose (including commercial) in favor of anyone who has lawful access to the works, but in this case the rights

		holders may opt-out (reserve) by contract or by a simple signal that excludes the work. In addition, the AI Italian Law introduced Article 70-*septies* to the Italian Copyright Law, which explicitly extends TDM exceptions to reproductions and extractions made using AI systems (including generative AI).
Does your jurisdiction have (1) an open, principle-based notion of "fair use" or (2) a closed, listed exceptions-based notion of "fair dealing"? Do those rules favor national players?	Fair dealing/ exceptions and limitations	The Italian and EU laws adopt an "exceptions and limitations" system. The exceptions are strict and established by law, meaning that if an activity does not fall within the exceptions provided by the laws, it cannot be carried out[246].
Have courts in your jurisdiction issued decisions on the application of "fair dealing" or "fair use" in relation to the use of unlicensed data to train AI models (i.e. via screen scraping)	No	N/A
Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?	Partially	Apart from the *sui generis* database right and the TDM exceptions, the Italian legal system provides - more generally - rules on intellectual and/or industrial property rights (within which those database and TDM-related provisions are situated) that can be indirectly linked, to some extent, to the notion of "data ownership" (*e.g.*, trade secrets), provided that all conditions are met. In addition, personal data protection rules may operate - to some extent - as a limitation on third-party access to, or use of, personal data.
Data Protection (Personal Information)		
What are the most notable data	Although there is no specific data	On the public-sector side: the Italian Cloud Strategy establishes a

[246] An example of exceptions established by the Italian laws are the TDM exceptions provided by Articles 70-*ter*, 70-*quarter*, and 70-*septies* of the Italian Copyright Law.

sovereignty/localization provisions applicable in your jurisdiction: c) in the public sector? d) in the private sector?	sovereignty/localisation regulation in Italy yet, the public and private sectors are following increasingly convergent rules.	data-localization-by-design model by virtue of which: (a) critical data must reside on infrastructure located in Italy; (b) strategic data must reside on EU-based cloud services; (c) ordinary data may also be hosted outside the EU as long as GDPR requirements are respected. This framework (rooted in the Italian Legislative Decree no. 82/2005 ("**Digital Public Administration Code**") and reinforced by regional practices) channels public data toward national or European infrastructures without formal prohibitions. On the private-sector side: supervisory bodies allow to use extra-EU cloud only with strict safeguards, while the Italian Data Protection Authority has increased its focus on transfers of personal data outside the European economic Area ("**EEA**") after the European Court of Justice, Case C-311/18 ("**Schrems II**")[247]. The overall effect is a *de facto* trend toward localization, driven not by explicit bans but by GDPR compliance and heightened scrutiny of transfers to third countries. In addition, apart from the GDPR, it is worth mentioning the following EU provisions which regulate, *inter alia*, the free movement of personal data - e-Privacy Directive: processing of personal data in the electronic communication sector; it ensures the free movement of such data and of electronic communication equipment and services in the EU; - Regulation (EU) 2018/1725: specific regulation for the processing activities of personal data carried out by the Union institutions, bodies, offices and agencies and on the free movement of such data.
What are special	Classified information /	Italy adopts data security classifications

[247] See the full text: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=11388612.

classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?	Unclassified but protected information	similar to the NATO/EU standard.
		In particular, for the public sector, the Prime Ministerial Decree no. 5/2015 distinguishes between:
		- classified information: sensitive information categorized, depending on its level of importance, as follows:
		  Highly Secret (SS);
		  Secret (S);
		  Highly Confidential (RR),
		  Confidential (R);
		- unclassified but controlled information (*e.g.*, for the "internal use"): unclassified information which, due to its sensitivity, requires minimal protection measures; and
		- exclusive dissemination information: information whose dissemination is limited to Italy alone, together with or without one or more foreign countries, for reasons of protecting strategic national interests and relations with foreign countries, by limiting access to information to persons who are Italian citizens only, together with or without persons who are citizens of one or more foreign countries only, by indicating "EXCLUSIVE ITALY" or "EXCLUSIVE ITALY and (name of the foreign country or countries)".

What are the most notable cross-border data transfer restrictions in your jurisdiction?	As an EU Member State, Italy strictly applies the GDPR and its provisions on the transfer of personal data outside the EEA	Chapter V of the GDPR (Articles 44 et seq.) is entirely dedicated to the transfer of personal data outside the EEA. Specifically, the GDPR provides that personal data may be transferred outside the EEA only under recognized safeguards (such as an adequacy decision from the European Commission, Standard Contractual Clauses ("**SCCs**"), Binding Corporate Rules ("**BCRs**"), or approved codes/certifications

		with binding commitments). Where no such safeguards exist, only the limited derogations under Article 49 GDPR apply (*e.g.*, explicit data subject's consent, the performance of a contract, public interest, legal claims, or vital interests).
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?	(1) *Schrems II* (2) *Commission Implementing Decision EU 2023/1795 on the adequate level of protection of personal data under the EU-US Data Privacy Framework* (3) *Cass. Civ., Sez. I, Ord., 13/05/2024, n. 12967*	(1) With this decision, the CJEU declared invalid the Implementing Decision (EU) 2016/1250 on the adequate level of protection of the EU-US Privacy Shield, finding that such framework did not ensure a level of data protection essentially equivalent to that required within the EU under Article 45 GDPR. As for Decision 2010/87/EU on SCCs, the CJEU did not invalidate it but imposed more stringent obligations on controllers and data exporters relying on such clauses. The Schrems II ruling further strengthened the role of national data protection authorities, holding that, in the absence of a valid adequacy decision, they must suspend or prohibit transfers based on SCCs where they consider that the clauses cannot be complied with in the third country and that the level of protection required by EU law cannot be ensured by other means. (2) After Schrems II, on 10 July 2023 the European Commission adopted its Implementing Decision about the EU-US Data Privacy Framework[248]. The European Commission has found that the U.S. now provides a level of data protection "essentially equivalent" to that of the EU, following significant reforms in U.S. law. New safeguards have been introduced to limit U.S. intelligence agencies' access to data to what is strictly necessary and proportionate. In addition, a two-tier redress mechanism has also been established, including the new Data Protection Review Court, which EU citizens can access. The European Commission decision provides for periodic reviews to ensure of the that these safeguards remain effective

[248] See the full text: https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng.

		over time. (3) The case concerned the validity of a data transfer agreement based on SCCs, in which the technical and organizational security measures were not described in detail within the agreement or its annexes, but were accessible via a reference to an external document published on the supplier's website. The Supreme Court (*Corte di Cassazione*) ruled that such a generic reference is not sufficient to meet the adequacy requirements. In addition, it stated that security measures must be an integral part of the contract, clearly identified and signed by the parties. In particular, the Supreme Court emphasized that SCCs not only regulate the relationship between the contracting parties (exporter and importer), but also create rights for the data subject, who acts as a third-party beneficiary. In this respect, the Supreme Court underlined that these rights would be nullified if the security measures were not objectively defined and could be unilaterally modified by the supplier without formal renegotiation.
Information Security Laws for critical infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	No Italy does not currently have a standalone national law specifically regulating information security for critical infrastructure. Instead, obligations for critical sectors are primarily implemented through EU framework	National and EU framework regarding critical infrastructure includes laws, directives and regulations such as: - Directive (EU) 2022/2555 ("**NIS2 Directive**")[249], setting cybersecurity requirements for operators of essential services and important entities across sectors, replacing the previous Directive (EU) 2016/1148 (NIS1 Directive) and implemented into national Law 138/2024; - CER Directive, that extends the protection of critical infrastructure, and it promotes resilience and adaptation to emerging threats; - Regulation (EU) 2024/2847 ("**Cyber**

[249] See full text of the directive https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555

		Resilience Act" o "**CRA**")[250], which imposes cybersecurity requirements for products with digital elements placed on the EU market. - Decree-Law No. 105 of 21 September 2019 ("**Cybersecurity National Perimeter Decree**"): it established the so-called National Cybersecurity Perimeter, identifying public and private entities operating in strategic sectors (energy, transport, finance, healthcare, etc.) that are required to comply with specific security obligations, incident-notification duties, and supplier-vetting requirements. The Perimeter strengthens the protection of national critical infrastructure against cyber threats, going beyond the safeguards provided under EU law.
In your jurisdiction, can directors and officers be held accountable for not diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?	No	Under Italy's NIS2 implementation (Legislative Decree 138/2024), boards/management must ensure robust cybersecurity risk management that addresses supply-chain dependencies and single points of failure. While NIS2 does not use the word "diversification," persistent, unjustified reliance on a single critical supplier can be treated as a breach of statutory cyber-risk management duties, leading to orders and administrative fines against the entity.
Lawful Access (Legal access to data without consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the	**Examples:** Italian Criminal Procedural Code, artt. 266-271	In Italy, intercepting private communications directly affects the right to freedom and confidentiality of correspondence and all other forms of communication, as protected by Article 15 of the Italian Constitution. This article guarantees the inviolability of correspondence and communications, allowing limitations only through a reasoned decision by a judicial authority, as set out in law. Interceptions are permitted only for specific categories of crime

[250] See the full text of the regulation https://eur-lex.europa.eu/eli/dir/2022/2557/oj

consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?		(determined by the seriousness of the penalty or the legal interest involved, see Article 266 of the Criminal Procedure Code). In accordance with Article 15, paragraph 2, interception require prior authorization from the judicial authority. Although the Public Prosecutor ("**PM**") initiates the request, but the power to authorize rests with the Judge for Preliminary Investigations ("**GIP**") under Article 267 of the Criminal Procedure Code. Furthermore, Italy does not permit foreign authorities to obtain data directly from Italian providers without employing formal legal cooperation mechanisms: a foreign authority must request assistance from its Italian counterpart. However, this process is often slow. To streamline the process, Italy has joined international instruments, such as the Budapest Convention on Cybercrime (2001) and the relevant Second Additional Protocol (2022) on enhanced cooperation and the disclosure of electronic evidence[251].
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a "collect all" regime) under such lawful access regime?	No	Under Italian law, lawful access to data without consent is strictly targeted and must be authorized by the GIP on the request of the PM. Interceptions and data access must specify the individuals involved, the methods, and the duration, and are allowed only when strictly necessary for the investigation. There is no legal framework in Italy that permits bulk data collection or "collect all" regimes.
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?	No	Under Italian law, lawful access to data without consent always requires judicial authorization. Interceptions and access to personal data must be approved by the GIP upon request of the PM. In exceptional urgent cases, the prosecutor may order immediate access, but must notify the GIP within 24 hours, and the authorization must be validated within 48 hours.

[251] See "*Reati informatici, più facile cooperare e condividere le prove: le novità dopo la firma del protocollo della Convenzione di Budapest*", Agenda Digitale, last updated 13 May 2022, available at https://www.agendadigitale.eu/sicurezza/cybercrime-piu-facile-cooperare-e-condividere-le-prove-le-novita-dopo-la-firma-del-protocollo-della-convenzione-di-budapest/#:~:text=Ratificato%20dall%E2%80%99Italia%20il%20secondo%20protocollo,prove%20elettroniche%3A%20Ecco%20cosa%20cambia.

Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Yes Examples: (1) European Investigation Order ("**EIO**"), established by Directive 2014/41/EU (2) Regulation (EU) 2016/794 (the "**Europol Regulation**") (3) National Procedures for Mutual Assistance in Criminal Matters ("**MLAT**"-s) with different States	(1) The EIO is a judicial decision issued or validated by a judicial authority in one EU country, authorising the carrying out of investigative measures to gather or use evidence in criminal matters in another EU country. It is valid throughout the EU, except in Denmark and Ireland. The EIO is based on mutual recognition, meaning the executing authority must recognise and ensure the execution of the other country's request; (2) Italian authorities also share data through Europol under the Europol Regulation[252], which facilitates cross-border police cooperation while ensuring compliance with national and EU data protection rules; (3) for example, Italy has signed an MLAT with the United State of America[253]
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation? What is their most notable impact on promoting technological autonomy?	Italian Law no. 287 of 1990 - "Rules for the protection of competition in the market" and Articles 101 and 102 of the Treaty on the Functioning of the European Union ("**TFUE**") and Regulation (EC) 1/2003 and the Consolidated text of the 1° July 2009 (indirectly, also the Directive	Italian Law No. 287 of 1990 ("**Italian Antitrust Law**") is the main statutory regime in Italy designed to promote competitive markets for innovation. It implements Article 41 of the Italian Constitution, safeguarding the freedom of economic initiative and ensuring that markets remain open and contestable. The Italian Antitrust Law aims to prevent exclusionary practices, abuses of dominant positions, and concentrations that could hinder the entry of new operators or obstruct the development of alternative technologies[255]. In addition, Italy is fully integrated into the wider EU competition framework. The substantive rules under Articles 101 and 102 TFEU, together with their enforcement system established by Regulation (EC) no.

[252] See the consolidated text here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0794-20220628
[253] See the full text here: https://www.state.gov/wp-content/uploads/2019/02/85-1113-Italy-Mutual-Legal-Assist-Treaty.pdf
[255] Law no. 287 of 1990, https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1990-10-13&atto.codiceRedazionale=090G0340

	2005/29/EC[254]) and Regulation (UE) 1925/2022 (Digital Market Act - "**DMA**")	1/2003, constitute the core of the EU competition regime by prohibiting anti-competitive agreements and market-foreclosing conduct. Although these rules are not explicitly aimed at promoting technological autonomy, they play an essential indirect role by preserving contestability and preventing dominant players from suppressing innovation. More directly, the DMA has a significant impact on technological autonomy. By imposing obligations on gatekeepers[256] and limiting structural dependencies on large global platforms, the DMA enhances the ability of EU (and consequently Italian) firms to develop and scale their own digital and technological solutions. It reduces lock-in effects, fosters interoperability, and promotes a more balanced digital ecosystem in which innovation can emerge from a broader set of players.
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?	Yes	These laws are actively applied by both courts and regulatory authorities in Italy, particularly by the Italian Antitrust Authority ("**AGCM**" or "**Authority**") which is responsible for protecting competition, addressing unfair practices, and supervising the conduct of dominant digital platforms. These functions require the Authority to apply the relevant regulatory framework, including the rules described above. One of the most recent measures adopted in this context by a regulatory authority concerns the provision adopted by the AGCM with respect Alphabet Inc. and Google Ireland Limited (collectively

[254] The Unfair Commercial Practices Directive 2005/29/EC may also play a marginal role, indirectly supporting trust and transparency in the internal market.

[256] Under the DMA, "gatekeepers" are large digital platforms holding a structurally dominant position in one or more digital markets, such as search engines, app stores, social networks, or online marketplaces. They are identified based on objective criteria, including annual EU turnover, number of active users, or number of business clients. Designated gatekeepers must ensure interoperability, fair access to services and data, and avoid self-preferencing practices. By regulating gatekeepers, the DMA promotes a more contestable digital ecosystem, enabling European and Italian companies to innovate and strengthen technological autonomy.

		"**Google**")[257]. Following the preliminary investigation, the AGCM required Google to: - redesign its consent form; - provide clearer information on the use of users' personal data and on the variety and quantity of Google services (including AI services, *e.g.*, Gemini) for which there may be a "combined" and "cross-referenced" use of personal data if consent is given; and - allow granular choices regarding data processing and service integration. At EU level, the Court of Justice of the European Union ("**CJEU**") has contributed to strengthening the competitive environment necessary for technological autonomy through landmark rulings interpreting Articles 101 and 102 TFEU. Although not expressly aimed at promoting technological sovereignty, decisions such as *Microsoft* (T-201/04)[258], *Google Shopping* (Case AT.39740, upheld in Case

[257] See the press release and the relevant AGCM's provision https://www.agcm.it/media/comunicati-stampa/2025/11/PS12714-.

[258] Microsoft Corp v. Commission of the European Communities is a case brought by the European Commission of the EU against Microsoft for abuse of its dominant position in the market. It started in the 1993, when Sun Microsystems form a complaint over Microsoft's licensing practices and resulted in the EU ordering Microsoft to divulge certain information about its server products and release a version of Microsoft Windows without Windows Media Player. See the full decision here https://curia.europa.eu/juris/document/document.jsf?text=&docid=62940&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10921202

		T-612/17)[259], and *Intel* (C-413/14 P)[260] have clarified the limits of dominant firms' conduct in digital and innovation-driven markets.
Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes")?	No	Italy has not entered into any bilateral free trade agreements that directly constrain or protect technological autonomy. Under Article 207 TFEU, the EU has exclusive competence over the common commercial policy. As a result, Italy participates exclusively in EU-negotiated free trade agreements ("**FTA**") and does not conclude its own.
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	No, Italy does not have formal "buy local" procurement rules due to EU law constraints. However, it has several instruments that functionally operate as a special type of "buy local" in high-tech and strategic sectors.	Although there are no formal 'buy local' procurement rules in Italy due to constraints imposed by EU law, several mechanisms effectively support national technological capabilities in advanced sectors. - the Golden Power regime[261] enables the government to review or block foreign acquisitions of strategic assets, including high-tech areas such as aerospace, cybersecurity, and artificial intelligence, thereby safeguarding

[259] Google v European Commission is a cause a case brought by the European Commission of the EU against Google LLC and Alphabet Inc. for abuse of its dominant position by favoring its own comparison-shopping service over competitors, reducing their visibility and traffic, in breach of Article 102 TFUE. Regarding so, The CJEU on 10 September 2024 upheld the European Commission's €2.42 billion fine against Google and its parent company Alphabet. The Court also rejected Google's challenge that the Commission should have applied the as-efficient-competitor (AEC) test, clarifying that Article 102 TFEU aims to protect competition, not less efficient competitors. In this case, the efficiency of rival comparison shopping services depended almost entirely on traffic diverted by Google, so the AEC test would not have provided reliable results, as Google's conduct had hindered competitors' ability to compete effectively. See the full decision here https://curia.europa.eu/juris/document/document.jsf?text=&docid=289925&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1326284

[260]Intel Corporation inc v European Commission is a cause brought by the European Commission of the EU against Intel for abuse of its dominant position by offering conditional rebates to four computer manufacturers and the European distributor Media-Saturn-Holding (MSH): *(i)* requiring that they purchase all or nearly all of their x86 microprocessor needs from Intel, and *(ii)* paying MSH on the condition that it sold only computers with Intel x86 processors. See the full decision here https://curia.europa.eu/juris/document/document.jsf?text=&docid=194082&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10915483

[261]See the full text of the communication here https://www.affarieuropei.gov.it/it/comunicazione/europarole/golden-power/

		domestic technological know-how; - similarly, the L. 89/2025 establishes a regulatory framework that supports national operators through authorizations, funding for innovation, and prioritization of Italian Small and Medium-sized Entreprises in space-related projects; - other instruments, such as law 808/1985 (regarding the measures for the development and growth of competitiveness of industries operating in the aeronautical sector) and PNRR programs, provide targeted support to domestic firms in aerospace, defense, and other high-tech sectors, fostering research and development while promoting industrial participation in strategic initiatives; - pre-commercial procurement (PCP)[262] and innovation-oriented public procurement further stimulate Italian companies to develop and deploy advanced technologies by offering project-based opportunities within a controlled regulatory framework. Moreover, Italy's participation in ESA operates under the geographical return principle, which redistributes contracts to national industry in proportion to each member state's contribution. While not a domestic law, this mechanism effectively channels investment into Italian enterprises and complements national efforts to strengthen technological autonomy.
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these	Yes Examples: (1) Patent Box (Article	(1) The Patent Box is an optional tax relief scheme linked to expenses incurred in carrying out research and development activities in relation to copyright-protected software, industrial patents, and legally protected designs and models. Such

[262] PCP is an approach to public procurement of research and development services that is outlined in the COM(2007) 799

incentives impose restrictions on origin of the funds and the manner in which they are invested?	146 Law Decree no. 146/2021) (2) Tax credit measure for research and development, technological innovation, design, and aesthetic conception[263]	measure is available to all business income earners, regardless of their legal status, size, or sector of production, including permanent establishments in Italy of residents in countries with which a double taxation agreement is in force and with which the exchange of information is effective. (2) The measure aims to support the competitiveness of businesses by stimulating investment in research and development, technological innovation, including in the context of Industry 4.0 and the circular economy, design, and aesthetic conception. Specifically: - for "general" technological innovation, the tax credit is granted at 10% until 2023 and at 5% from 2024 to 2025, with an annual cap of 2 million euros. - for 4.0 and green technological innovation, the rate is 15% until 2022, decreasing to 10% in 2023 and to 5% for 2024-2025, with an annual cap of Euro 4 million. The percentages apply to the calculation base net of any other subsidies or contributions received.
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?	No	N/A
Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues	Yes (1) Proposal for a Regulation on simplification of the digital legislation	(1) On 19 November 2025, the European Commission published the final version of the Digital Omnibus Package, which aim to simplify and streamline the EU's digital regulatory framework. The COM(2025) 837 has a cross-cutting

[263] See the Minister of the Enterprises and Made in Italy's explanation of the measure https://www.mimit.gov.it/it/incentivi/credito-d-imposta-r-s.

related to technological autonomy?	(COM(2025) 836[264] and COM(2025) 837[265], presented jointly as part of the "**Digital Omnibus Package**") (2) Proposal for a regulation on the safety, resilience and sustainability of space activities in the EU (COM(2025) 335[266] or "**EU Space Act**")	impact on all EU regulations concerning data, technologies, digital services, and cybersecurity, while the COM(2025) 836 introduces targeted amendments to the AI Act to ensure its clearer, simpler, and more innovation-friendly application. The Digital Omnibus Package is the first step in the EU digital regulatory simplification strategy, which aims to reduce administrative burdens, eliminate regulatory overlaps, and improve legal certainty in an increasingly complex regulatory ecosystem. (2) On 25 June 2025, the European Commission published the final version of the proposal of the EU Space Act. The EU Space Act aims to harmonize the regulatory framework for space activities across the EU, strengthening the capabilities of member states and fostering a competitive and autonomous European space sector. Italy's alignment with this framework will likely reinforce domestic participation in strategic space projects.

[264] See the full text of the proposal here https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal
[265] See the full text of the proposal here https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal
[266] See the full text of the proposal here https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0335

Norway

Kristian Foss, Advokatfirmaet Bull AS, Norway

Executive summary

Norway faces a complex landscape in its pursuit of national technological autonomy. A key concern is the country's **reliance on foreign-owned cloud and digital platforms**, which raises issues of data sovereignty and compliance with strict privacy regulations such as GDPR. Norwegian enterprises often struggle to ensure that sensitive data remains within national borders, particularly when using global cloud providers, creating legal and operational challenges. Additionally, **hybrid threats**—combining cyberattacks, disinformation, and influence operations—pose risks to Norway's digital infrastructure and public trust, as highlighted by the Norwegian Police Security Service. These vulnerabilities underscore the difficulty of achieving full control over critical technologies and information flows in an interconnected global environment.[267]

Despite these challenges, Norway has notable **strengths**. The country is among the most digitalized in Europe, supported by world-class infrastructure and high digital literacy. Norway's vibrant startup ecosystem, backed by Innovation Norway and programs like SkatteFUNN, fosters innovation in artificial intelligence, cleantech, and advanced computing. These efforts position Norway as a leader in responsible AI development and as an emerging player in quantum technology, with significant investments announced to strengthen national capacity.[268]

Technological autonomy policies are most visible in sectors critical to national security and competitiveness, including telecommunications, financials, cybersecurity, and green technology. Norway's digitalisation strategy emphasizes secure ICT services, resilient infrastructure, and reduced dependency on foreign providers, aligning with broader European efforts to safeguard digital sovereignty. [269]

The technologies at the center of these policies include artificial intelligence, cloud computing and increasingly quantum technologies. AI governance is being reinforced through the preparations for the implementation of the EU AI Act[270], while quantum computing and secure communication are prioritized under a dedicated national strategy. In addition, Norway aims to become the world´s most digitalised country by 2030, and will therefore introduce its own law regulating artificial intelligence. This law implements the EU´s AI Act.[271] These focus areas

[267] Dev Centre House Ireland, *Data Sovereignty Concerns in Norway´s Cloud Strategy, (November 2025),* https://www.devcentrehouse.eu/blogs/data-sovereignty-concerns-in-norways-cloud-strategy/
[268] Kongsberg Group, *A leap for quantum technology in Norway,* (August 2025), https://www.kongsberg.com/newsroom/stories/2025/8/A-leap-for-quantum-technology-in-Norway/
[269] Norwegian Ministry of Digitalisation and Public Governance*, The Digital Norway of the Future: National Digitalisation Strategy 2024–2030*, (October 2024), https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/en-gb/pdfs/digitaliseringsstrategi_eng.pdf
[270] Government of Norway, Paving the way for safe and innovative use of AI in Norway, (March 2025), https://www.regjeringen.no/en/whats-new/gjor-norge-klar-for-trygg-og-innovativ-ki-bruk/id3093081/
[271] The Government, *Lov om kunstig intelligens i Norge sendes nå på høring*, (June 2025), https://www.regjeringen.no/no/aktuelt/lov-om-kunstig-intelligens-i-norge-sendes-na-pa-horing/id3113732/

<table>
<tr><td colspan="3">reflect Norway's ambition to maintain competitiveness and security in a rapidly evolving global tech environment.[272]</td></tr>
<tr><th colspan="3">Defining Technological Sovereignty</th></tr>
<tr><td>How is technological sovereignty defined in your jurisdiction? What are the most important factors considered?

Examples of Factors:
● Political
● Social
● Dependency perspective
● IT Infrastructure
● Legislative perspective (various levels)</td><td colspan="2">Technological sovereignty requires national control over ICT services and infrastructure, as stated by the Norwegian National Security Authority (NSM), and is defined as ensuring that critical ICT assets are under actual technical and legal Norwegian control, so that one can be reasonably certain no foreign company or government has any form of technical access. This is essential to protect the nation and citizens´ rights. [273]</td></tr>
<tr><th colspan="3">Cloud Sovereignty</th></tr>
<tr><td>Has your jurisdiction published a national cloud sovereignty policy?</td><td>No</td><td>Explanation:

Norway has not published a dedicated national cloud sovereignty policy. However, Norway has addressed sovereignty concerns through related strategies and regulations, primarily in three areas:
(1) Cloud Computing Strategy for Norway:
● The strategy sets out principles for secure and lawful use of cloud services, but does not mandate a sovereign cloud model.(source)</td></tr>
</table>

[272] Simula, *QIT Norway 2025 and the national quantum strategy,* (May 2025), https://www.simula.no/about/news/qit-norway-2025-and-national-quantum-strategy

[273] The Norwegian National Security Authority (NSM), *Report: National Control For ICT Services*, (November 2024) p. 6, https://nsm.no/getfile.php/1314066-1731394410/NSM/Filer/Dokumenter/Rapporter/National%20Control%20for%20ICT%20services.pdf

		● The strategy also emphasizes risk assessment, information security, and contractual safeguards for cloud adoption.[274] **(2) NSM Report: National Control for ICT Services:** ● NSM provides guidance on national control for ICT services, which includes cloud services. The report mentions factors for national control, and these principles aim to reduce foreign dependencies for critical services.[275] **(3) The Data Centre Industry Strategy:** ● The Data Centre Industry Strategy emphasizes that critical societal functions should be delivered from data centers in Norway or allied countries. It also sets security requirements for data centers and highlights their role in strengthening national and regional digital autonomy.[276] **(4) National Strategy for Artificial Intelligence :** ● Norway's national AI strategy aims to use AI to drive

[274] Government of Norway, *Cloud Computing Strategy for Norway*, (June 2016) p. 10-16, https://www.regjeringen.no/en/documents/cloud-computing-strategy-for-norway/id2484403/?ch=5

[275]The Norwegian National Security Authority (NSM), *Report: National Control For ICT Services*, (November 2024),

https://nsm.no/getfile.php/1314066-1731394410/NSM/Filer/Dokumenter/Rapporter/National%20Control%20for%20ICT%20services.pdf

[276] Norwegian Ministry of Digitalisation and Public Governance, *The Data Centre Industry Strategy*, (October 2025) p. 33-38, https://www.regjeringen.no/contentassets/dff2f4dc656043be9ad5837ebbca6fae/en-gb/pdfs/datasenternaeringa-strategi-eng.pdf

		innovation, value creation and better public services, while protecting human rights, privacy and security. It focuses on building data, skills and research capacity, and ensuring that AI is developed and used in a responsible, human-centric and trustworthy way.[277] These measures aim to ensure that sensitive data and critical services remain under Norwegian or allied control, without mandating a fully sovereign cloud model.
AI and Technology Sovereignty policy		
Has your jurisdiction published a national technology sovereignty policy?	No	**Explanation:** Norway has not published a dedicated national technology sovereignty policy. Instead, sovereignty principles are embedded in broader strategies and guidelines related to digitalization and ICT security. **(1) National Digitalisation Strategy:** ● The strategy does not use the term “technology sovereignty” explicitly, but it emphasizes that Norway must “take the helm and steer the course of [technology´s] development” so that technology serves society rather than controls it.[278]

[277] The Government, *National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

[278] Norwegian Ministry of Digitalisation and Public Governance, *The Digital Norway of the Future: National Digitalisation Strategy 2024-2030*, (October 2024) p. 3, https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/en-gb/pdfs/digitaliseringsstrategi_eng.pdf

		(2) NSM Report: National Control for ICT Services: ● The NSM Report provides the clearest official guidance on sovereignty-related issues and provides sovereignty-related principles for ICT services.[279]
Does your jurisdiction have a published national AI strategy/policy?	Yes	**Explanation (e.g. top 3-5 priorities):** ● Ethical and trustworthy AI.[280] ● World-class AI infrastructure.[281] ● Innovation and value creation.[282] ● Data management and sharing.[283]
Does your jurisdiction have a published AI compute or cloud strategy/policy?	**AI compute strategy/policy:** ● No **AI cloud strategy/policy:** ● No	**Explanation:** **AI compute strategy/policy:** Norway does not have a standalone national AI compute strategy. However, compute capacity is addressed as a priority within the National Strategy for Artificial Intelligence and through recent high-performance computing (HPC) investment plans. ● **National AI strategy:** The strategy explicitly states that the Government will "facilitate world-class AI infrastructure in Norway in the form of digitalisation-friendly regulations,

[279]The Norwegian National Security Authority (NSM), *Report: National Control For ICT Services*, (November 2024) p. 10-16, https://nsm.no/getfile.php/1314066-1731394410/NSM/Filer/Dokumenter/Rapporter/National%20Control%20for%20ICT%20services.pdf
[280]Government of Norway, *The National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=7
[281]Government of Norway, *The National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=2
[282] Government of Norway, *The National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=2
[283] Government of Norway, *The National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=2

		good language resources, fast and robust communication networks, and sufficient computing power".[284] ● **HPC?? Investment Plan:** The Norwegian Research Council recommended investing 3.4 billion NOK in supercomputing infrastructure to meet growing computational needs for research and AI. The plan designates Sigma2 as the sole provider of HPC infrastructure for research and public sectors, aiming to strengthen Norway's competitiveness and innovation capacity.[285] **AI cloud strategy/policy:** Norway does not have a standalone AI cloud strategy or policy. However, cloud-related provisions appear in the National Strategy for Artificial Intelligence[286], Cloud Computing Strategy for Norway[287] and the Norwegian AI Cloud (NAIC) Initiative.[288]
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks	Yes	**Explanation:** Digital sovereignty is in Norway a hotly debated issue, in the press, social media, seminars etc.. It is also a major public concern. On 27 – 31 October Norway hosted the International Conference on Digital Sovereignty. [289]

[284] Government of Norway, *The National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=2
[285]Sigma2, *How Norway will spend 3.4 billion NOK on supercomputing*, (January 2025), https://www.sigma2.no/news/2025/how-norway-will-spend-34-billion-nok-supercomputing
[286]Government of Norway, *The National Strategy for Artificial Intelligence*, (January 2020), https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=2
[287]Government of Norway, *Cloud Computing Strategy for Norway*, (June 2016), https://www.regjeringen.no/en/documents/cloud-computing-strategy-for-norway/id2484403/?ch=2
[288] NAIC, *Norwegian AI Cloud: About,* https://www.naic.no/english/about/index.html
[289] IFE, *2nd International Conference on Digital Sovereignty (ICDS) 2025*, (September 2025), https://ife.no/en/event/international-conference-on-digital-sovereignty-icds-2025/

related to technological sovereignty?		The event featured Norway´s Minister of Digitalisation and Public Governance as a keynote speaker and covered topics like secure data spaces, autonomous cloud services, and governance, indicating government engagement and expert debate.
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	Yes	**Explanation:** Norway has developed foundational AI models, primarily large language models (LLMs), through collaborations between research institutions, public sector bodies, and private companies.[290] ● **NorLLM (Norwegian Large Language Models:** This is developed by NorwAI, a national research center led by NTNU. The goal is to provide open, Norwegian-trained models for public and private use to reduce dependency on foreign tech giants.[291] ● **University of Oslo** ● **National library**
Does your jurisdiction have national AI research centres of excellence?	Yes Examples : (1) NorwAI – Norwegian Research Center for AI Innovation	**Explanation:** Links to AI research centres of excellence: (1) NorwAI: https://www.ntnu.edu/norwai (2) NORA: https://www.nora.ai/

[290]AIavisen, Norske språkmodeller: Dette er de 3 viktigste initiativene (May 2024), https://aiavisen.no/norske-sprakmodeller/
[291]NorwAI – Norwegian Research Center for AI Innovation, A guide to NorwAI´s work on Large Language Models in Norwegian, https://www.ntnu.edu/norllm

	(2) NORA – Norwegian Artificial Intelligence Research Consortium	Also, Norway has established the Artificial Intelligence Initiative that aims to increase "research efforts on artificial intelligence and digital technologies by at least one billion over the next five years." [292] Six national research centres on artificial intelligence will commence operations in 2025.[293] Still, when we look at the funding compared to other countries, the initiatives look defensive.
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes	**Explanation:** Norway has active research and development capacity in quantum computing and related technologies, supported by national infrastructure projects, research centres, and competence building. ● **National Research Infrastructure and Funding:** In June 2025, the Norwegian government allocated NOK 43 million to strengthen quantum technology research infrastructure.[294] ● **Research Centres:** The Gemini Center on Quantum Technology (SINTEF, NTNU, UiO) coordinates research on quantum computing, aiming to secure Norway´s position as a key player in future technology landscapes. [295] ● **Competence Building:** The Research Council of Norway launched a call for proposals to establish national research centres

[292] The Research Council of Norway, The Artificial Intelligence Initiative, https://www.forskningsradet.no/en/research-policy-strategy/ltp/artificial-intelligence/
[293] The Research Council of Norway, *The Norwegian government's billion-kroner investment: These are Norway's six new research centres for artificial intelligence*, (September 2025), https://www.forskningsradet.no/en/news/2025/artificial-intelligence/
[294] Government of Norway, 43 millioner kroner til satsing på kvanteteknologi, (June 2025), https://www.regjeringen.no/no/aktuelt/43-millioner-kroner-til-satsing-pa-kvanteteknologi/id3109876/
[295] SINTEF, Opening of the Center for Quantum Technology, (January 2025), https://www.sintef.no/en/latest-news/2025/opening-of-the-center-for-quantum-technology/

		for quantum technology, with up to 244 million.[296]
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech stack, funding and adoption: 1. AI compute (GPU equipped) data centres 2. Domestically developed AI foundational models 3. Existence of large high-value databases in high-value sectors of economic activity 4. Availability of funding/financing for commercialization of innovation 5. Rates of AI adoption 6. Domestic quantum computing research, development and commercialization 7. Domestic military defense industry	**Please rate each component on a five point scale and circle the best option** (1 = non-existent; 2 = nascent; 3 = existing but insufficient; 4 = solidly in place; 5 = world leading): **1. AI compute (GPU-equipped) data centres** 1 2 3 4 5 **2. Domestically developed AI foundational models** 1 2 3 4 5 **3. Existence of large high-value databases in high-value sectors of economic activity** 1 2 3 4 5 **4. Availability of funding/financing for commercialization of innovation** 1 2 3 4 5 **5. Rates of AI adoption by organizations** 1 2 3 4 5 **6. Domestic quantum computing research, development and commercialization** 1 2 3 4 5	
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	Yes	Norway implemented the EU Database Directive (directive 96/9/EC) through its Copyright Act.[297] It provides special legal protection for databases beyond basic copyright through the sui generis database right, implemented under the EU Database Directive. This grants the maker of a database exclusive rights to prevent extraction and reuse of

[296]The Research Council of Norway, Centre for Quantum Technology Research, (July 2025), https://www.forskningsradet.no/en/call-for-proposals/2025/centre-quantum-technology-research/
[297] Intellectual Property Act, Act No. 40 of June 15, 2018

		substantial parts of its content for 15 years, provided there was substantial investment in obtaining or presenting data.[298] Norway does not grant general ownership rights over raw data outside these frameworks, but do mind the EU Data Act, that is still not transposed to Norwegian law.
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?	No	Norway is in the process of implementing the EU Directive on Copyright in the Digital Single Market (Directive 2019/790) into its Copyright Act (Åndsverkloven). The proposed amendments provide that reproduction of protected works for TDM is permitted without the rightholder´s consent, provided the user has lawful access to the data.[299] Norway also promotes research and commercialization through the Research and Innovation Department. This department develops policies for industrial research and development and commercialization, including grants to the Research Council of Norway, Innovation Norway, and others.[300]
Does your jurisdiction have (1) an open, principle-based notion of “fair use” or (2) a closed, listed exceptions-based notion of “fair dealing”? Do those rules favor national players?	Nei	Norway follows an exceptions-based system similar to “fair dealing”, where permitted users are specifically listed in the Norwegian Copyright Act (Åndsverkloven). This means Norwegian law does not allow a general “fairness” test; only uses

[298] The European Union, Database protection, (November 2025), https://europa.eu/youreurope/business/running-business/intellectual-property/database-protection/index_en.htm
[299] Government of Norway, Digitalmarkedsdirektivet, (December 2023), https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2016/des/dsm-direktivet/id2556742/
[300] Government of Norway, *Research and Innovation Department*, https://www.regjeringen.no/en/dep/nfd/organisation/Departments/research-and-innovation-department/id528252/

		explicitly listed in the statute are permitted.[301] There is no evidence that these exceptions favor Norwegian entities over foreign ones. The rules apply equally to all users within Norway, regardless of nationality. The system is harmonized with EU law under the EEA Agreement, meaning Norway implements the same exceptions as EU member states. [302]
Have courts in your jurisdiction issued decisions on the application of "fair dealing" or "fair use" in relation to the use of unlicensed data to train AI models (i.e. via screen scraping)?	No No	Norwegian courts have not issued any decisions on the application of "fair dealing" in relation to the use of unlicensed data to train AI models, including practices such as screen scrapping.
Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?	Yes	Norway has implemented Directive 96/9/EC on the legal protection of databases into its Copyright Act (Åndsverkloven). This provides copyright protection for databases that are original, as well as a sui generis right for databases involving substantial investment in obtaining, verifying, or presenting contents (15-year protection). Beyond this, Norwegian law does not recognize "data ownership" as a property right. Instead, exclusivity arises in specific sectors or through EU-aligned frameworks[303]. For example, Norway is implementing the

[301] Copyright Act, Act No. 40 of June 15, 2018
[302] WIPO, Intellectual Property Act, Norway, (September 2021), https://www.wipo.int/wipolex/en/legislation/details/22504
[303] Government of Norway, *Marketing authorization of medicinal products*, (February 2024), https://www.regjeringen.no/en/topics/health-and-care/pharmaceuticals/innsikt/product-approval/id434890/

		EU Data Act on harmonised rules on fair access to and use of data.[304] In addition, in the pharmaceutical sector, Norway follows EU rules granting 8 years of data exclusivity and 10 years of market exclusivity for reference medical products under Directive 2001/83/EC and Regulation (EC) No 726/2004. Similarly, in the petroleum sector, interpreted geodata submitted to authorities is confidential for 5 years, and commercially available data for 10 years.[305] These rules do not favor Norwegian players; they apply equally to all entities within the EEA and EU.
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: e) in the public sector? f) in the private sector?	Public sector: (1) Cloud Computing Strategy for Norway (2) One Digital Public Sector Strategy (3) National Digitalisaion Strategy Private sector:	Norway´s public sector data sovereignty framework is anchored in three key strategies: (1) This establishes that public sector agencies must conduct information value assessments, risk assessments, and ensure information security before using cloud services. Sensitive or high-security data should remain under Norwegian jurisdiction. The strategy highlights legal uncertainties about storing personal data abroad and recommends contractual safeguards and coordination for secure data centers in Norway. [306]

[304] The Government, *Dataforordningen*, (October 2024), https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2022/sep/dataforordningen/id2928372/
[305] Norwegian Offshore Directorate*, Release of Data*, (July 2024), https://www.sodir.no/en/facts/data-and-analyses/release-of-data/
[306] Norwgian Ministry of Local Government and Modernisation*, Cloud Computing Strategy for Norway*, (June 2016) p. 13-16, https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

	(4) GDPR and Norwegian Personal Data Act (5) Digital Operational Resilience Act (DORA) (6) Digital Security Act	(2) The strategy mandates secure digitalization and cyber security integration in all public sector IT solutions. It require compliance with privacy and security standards. Cyber security is treated as a prerequisite for trust in the public sector´s IT systems and public digital services. [307] (3) The strategy emphasizes data sharing under EEA law, requiring that public sector data be managed in a way that respects security. It sets principles for data use: “open when possible and protected when necessary”, ensuring compliance with legal frameworks such as GDPR. [308] Explanation b): (4) Norway implements the General Data Protection Regulation (GDPR) through the Personal Data Act.[309] While GDPR does not impose strict localization, it restricts transfers of personal data outside the EEA unless adequate safeguards exist. [310] (5) This regulation require banks, insurance companies, and other financial entities to maintain control

[307] Ministry of Local Government and Modernisation, One Digital Public Sector: Digital Strategy for the Public Sector 2019-2025, (June 2019) p. 10 and 52-54, https://www.regjeringen.no/contentassets/db9bf2bf10594ab88a470db40da0d10f/en-gb/pdfs/digital_strategy.pdf

[308] Norwgian Ministry of Digitalisation and Public Governance, *The Digital Norway of the Future: National Digitalisation Strategy 2024-2030*, (October 2024) p. 63, https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/en-gb/pdfs/digitaliseringsstrategi_eng.pdf

[309] Personal Data Act, Act No. 38 of June 15. 2018

[310] AJ Richter, *Does Server Location Really Matter Under GDPR? Understanding Data Localization in the Context of Data Protection Compliance*, (July 2024), https://techgdpr.com/blog/server-location-gdpr/

		over ICT systems and outsourcing arrangements. While not an absolute localization mandate, these rules will often lead to data storage within Norway or the EU for critical financial data. [311] (6) The Digital Security Act applies to operators of essential services and digital service providers. It requires risk assessments, incident reporting and proportional security measures to prevent and mitigate cyberattacks.[312] For critical infrastructure and services, this often translates into keeping sensitive data within Norwegian or EEA jurisdiction to ensure compliance and resilience.
What are special classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?		Protected Information: (*Non-national security interest; harm to individuals or organizations if compromised*) ● Strictly in confidence ● In confidence The legal basis is the Information Protection Instructions Section 2, 9 and 12. This requires strict security controls.[313] Classified Information: (*National security interest; harm to Norway´s security or stability if compromised*)

[311] EIOPA, *Digital Operational Resilience Act (DORA),* https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[312] Bull, K. Foss & O. M. Moe & H. B. Olaussen, *Norway implements NIS1 from 2016 in extended version – in effect from 1 October 2025* (September 2025), https://www.bull.no/en/articles/technology-it-ai/norway-implements-nis1-from-2016-in-extended-version

[313] The Norwegian National Security Authority (NSM), *Instructions for the handling of records that need to be protected for reasons other than those set out in the Security Act and associated regulations (Information Protection Instructions)*, (July 1972), https://nsm.no/getfile.php/134012-1593765563/NSM/Filer/Dokumenter/a03---s-17-02014-1-for-1972-03-17-3352-beskyttelsesinstruksen_engelsk-oversettelse-465767_1_1.pdf

		• Restricted • Confidential • Secret • Top secret The Security Act requires information to be processed in approved secure facilities, cf. chapter 3-6. [314]
What are the most notable cross-border data transfer restrictions in your jurisdiction?	(1) GDPR and Norwegian Personal Data Act (2) Digital Operational Resilience Act (DORA)	(1) Transfers of personal data outside the EEA are only permitted if the destination country has appropriate safeguards in place. If this is not the case, the Norwegian organization that transfers personal information will be held accountable. [315] (2) Financial institutions outsourcing ICT services must comply with DORA requirements. Contracts must include audit rights, risk assessments, and operational resilience testing.[316]
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?	(1) Suspension of Data Transfers to Russia – Yango Case (2023) (2) Temporary Ban of Behavioral Advertising on Facebook and Instagram –	(1) The Norwegian Data Protection Authority imposed a temporary halt in Yango´s transfer of personal data from Norway to Russia in connection with the Yango taxi application. The decision cited GDPR Article 44 and Chapter V, stating that Russian law granting authorities broader access to passenger data undermined GDPR protections. The ban was issued

[314] Act relating to national security (Security Act) Act No. 24 of June 1. 2018
[315] (EU) 2016/679, General Data Protection Regulation (GDPR), Chapter V, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:32016R0679
[316](EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (December 2022) Article 28 to 30, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

	Meta Platforms (2023)	under the urgency procedure in Article 66. [317] (2) The Norwegian Data Protection Authority imposed a temporary ban on Meta´s behavioral advertising practices on Facebook and Instagram in Norway. The decision was based on GDPR violations, including lack of valid legal basis for processing personal data for targeted ads. While not a direct transfer case, it is highly relevant because Meta's ad systems involve cross-border data flows to the U.S and other jurisdictions, and the ruling emphasized the need to protect Norwegian user´s rights under GDPR.[318]
Information Security Laws for Critical Infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Yes (1) Digital Security Act (2) Security Act (3) Electronic Communications Act	(1) The Digital Security Act implements the EU NIS1 Directive, and applies to providers of essential services and certain digital service providers. Special considerations for providers are to establish and maintain a digital security management system, implement organizational, technical, and physical security measures proportionate to risk and report incidents to the Norwegian

[317]Norwegian Data Protection Authority, *Advance notification – Yango – Transfers of personal data to the Russian Federation*, https://www.datatilsynet.no/contentassets/229ffa763e7349dfbd00e16ca2772578/_-23_03080-1-yango-letter_final-419435_2_1.pdf

[318]Norwegian Data Protection Authority*, Temporary ban on behavioural advertising on Facebook and Instagram,* https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/temporary-ban-of-behavioural-advertising-on-facebook-and-instagram/

		National security Authority (NSM) without undue delay.[319] (2) The Security Act applies to governmental bodies and private undertakings designated as vital to national security. The law requires protective security measures for information systems and infrastructure critical to national functions, information security requirements for classified information and systems and ownership control for businesses critical to national security.[320] (3) The Electronic Communications Act introduces strict security obligations for telecom and data center operators, including number-independent communication services. The law requires that networks, services, and data centers maintain adequate security and preparedness in times of peace, crisis, and war, and ensure confidentiality, integrity, and availability of communication and data. The Act also introduces a registration obligation for data centers.[321]
In your jurisdiction, can directors and officers be held accountable for not	Yes	In Norway, directors and officers can be held personally liable for damages caused intentionally or negligently in

[319] Sicra: O. Skauge*, The Digital Security Act entered into force on October 1, 2025 – what does it mean for businesses**?***, (October 2025)*,* https://sicra.no/en/knowledge/blog/the-digital-security-act-entered-into-force-on-october-1-2025-what-does-it-mean-for-businesses

[320] Act relating to national security (security act) Act No. 24 of 1. June 2018, chapter 5, 6and 10, https://lovdata.no/dokument/NLE/lov/2018-06-01-24

[321] Electronic Communications Act, Act of 4th of July 2003 No. 83 § 3-7

diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?		their role. [322] In a 2016 case, the Court held that if "duties that objectively apply" are violated, there is a presumption of negligence. This means that if cybersecurity or supply chain security obligations apply and are breached, directors may be presumed negligent. [323] In addition, the EU NIS2 Directive is to be implemented in Norway. This means that essential and important entities must implement measures for "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers."[324] Also, management bodies must approve and oversee cybersecurity risk-management measures and can be held liable for non-compliance.[325] Norwegian law does not explicitly require diversification of digital infrastructure, but the duty to manage risk and ensure proper organization, NIS2´s supply chain security requirement, and the Supreme Court´s presumption of negligence, collectively create a framework where failure to mitigate supplier concentration or ensure resilience in critical digital infrastructure could expose directors and officers to personal liability.
Lawful Access (Legal Access to Data without Consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to	(1) The Intelligence Service Act chapter 7	(1) The Intelligence Service Act authorizes the Norwegian Intelligence Service to collect and process personal data for foreign

[322]Norwgian Limited Liability Companies Act, Act No. 44 of 13. June 1997 Article 17-1, https://lovdata.no/pro/#document/NL/lov/1997-06-13-44/%C2%A717-1

[323] Bull: K. Foss*, A stricter board responsibility for cyber security*, (May 2024), https://www.bull.no/en/articles/technology-it-ai/a-stricter-board-responsibility-for-cyber-security

[324](EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Article 21 (2) (d), https://eur-lex.europa.eu/eli/dir/2022/2555

[325](EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, Article 20 (1)-(2), https://eur-lex.europa.eu/eli/dir/2022/2555

personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?	(2) Electrnic Communications Act § 3-14 (3) Personal Data Act (GDPR implementation) GDPR Article 48 and 49	intelligence purposes without the consent of affected individuals, including bulk collection of cross-border electronic communications and targeted searches upon court approval. The Act does not grant foreign authorities direct lawful access, and any sharing of information must follow Norwegian law. (2) Mandates telecom providers to retain certain traffic and subscriber data and disclose it to law enforcement upon lawful request, without requiring user consent.[326] (3) Personal Data Act prohibits direct disclosure of personal data to foreign authorities unless based on an international agreement or other legal basis under EU/EEA law. Foreign authorities cannot obtain direct lawful access; transfers must follow GDPR safeguards.[327]
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a "collect all" regime) under such lawful access regime?	No	Norwegian law does not explicitly authorize bulk or indiscriminate transfers under lawful access regimes. Any such access must be grounded in a specific legal basis and comply with necessity and proportionality requirements.[328]
Do such regimes provide for the possibility of such lawful	No	Norwegian law does not permit a general "warrantless" or "no judicial

[326] Electronic Communications Act, Act No. 76 of 13. December 2024, https://lovdata.no/dokument/NL/lov/2024-12-13-76/KAPITTEL_3#%C2%A73-14
[327]Algolia, *GDPR Made searchable*, https://gdpr.algolia.com/gdpr-article-48
[328] Act relating to the processing of data by the police and the prosecuting authority (the Police Databases Act), Act No. 16 of 28. May 2010**,** https://lovdata.no/dokument/NLE/lov/2010-05-28-16 and Electronic Communications Act, Act No. 76 of 13. December 2024, https://lovdata.no/dokument/NL/lov/2024-12-13-76/KAPITTEL_3#%C2%A73-14 and Algolia, *GDPR Made searchable*, https://gdpr.algolia.com/gdpr-article-48

access without a warrant or judicial oversight?		oversight" regime for accessing personal data.[329]
Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Yes (1) Schengen Agreement (2) EU-US Data Protection Umbrella Agreement	(1) Norway participates in the Schengen Agreement, which enable police cooperation, information exchange, legal cooperation on criminal cases, visa and checks on persons at the external borders.[330] (2) This applies to Norway via EEA alignment. It sets privacy safeguards and judicial redress for law enforcement data transfers, reinforcing GDPR principles of necessity and proportionality.[331]
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation?What is their most notable impact on promoting technological autonomy?	*Norwegian Competition Act, Act 12 of 5. March 2004.* *Innovation Norway – a government-owned entity*	The purpose of the Act is to promote competition across all relevant markets,ensuring efficient resource utilization and consumer welfare. It prohibits anti-competitive agreements, abuse of dominance, and regulated mergers. The Act is fully harmonized with EU competition standards throughthe European Economic Area Agreement (EEA), meaning its framework is not uniquely Norwegian but aligned with European rules. [332] By preventing monopolistic practices and ensuring open markets, the Act creates conditions for new entrants and innovative firms to compete,

[329] Linklaters, *Data Protected – Norway*, (February 2024), https://www.linklaters.com/insights/data-protected/data-protected---norway

[330] Government of Norway, *Cooperation on Schengen and Justice and Home affairs*, (January 2025), https://www.regjeringen.no/en/topics/european-policy/Norways-relations-with-Europe/cooperation-schengen/id684929/

[331] European Parliament, Legislative Train Schedule, *Conclusion of the EU-US data protection umbrella agreement,* (October 2025), https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-conclusion-of-the-eu-us-data-protection-umbrella-agreement

[332] Norwegian Competition Authority, *Overview of Competition Legislation in Norway,* https://konkurransetilsynet.no/legislation/?lang=en

		reducing dependency on dominant players and foreign-controlled platforms. Innovation Norway is a government-owned entity and the Norwegian Government's main instrument for innovation and business development. It provides grants, loans, and guarantees to promote competitiveness, sustainability, and value creation. These measures constitute state aid and are regulated under the EEA Agreement's state aid rules, harmonized with EU law and enforced by the EFTA Surveillance Authority (ESA).[333]
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?	Yes	The Supreme Court overturned the Norwegian Competition Authority´s prohibition of Schibsted´s acquisition of Nettbil, a digital car auction platform. At the time, Nettbil was a newly established company with a small market share, while Schibsted controlled Finn.no, a classified advertising platform that held a dominent position in the car advertisement market. The Court emphasized that the Authority´s strict approach to blocking mergers could hinder innovation and market entry by startups. [334]
Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes")?	Yes (1) European Economic Area (EEA) Agreement (2) Extended Intelligence	(1) Norway is part of the EEA, which integrated it into the EU single market and subjects it to EU digital trade and data protection rules, including GDPR. These rules constrain unilateral data-sharing and require necessity,

[333] Innovation Norway, *National Legal Basis – ESA*, (June 2025), https://www.innovasjonnorge.no/artikkel/national-legal-basis-esa

[334] OsloEconomics, *Decision to block Schibsted/Nettbil merger overturned*, (March 2022),

	Cooperation (Nine Eyes)	proportionality, and safeguards for cross-border transfers. [335] **(2)** Norway is not a Five Eyes member but participates in the broader "Nine Eyes" alliance, which involves intelligence-sharing arrangements. These are not trade agreements but can indirectly affect technological autonomy by enabling surveillance cooperation.[336]
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	No	No explicit "buy local" requirement exists for advanced technology equipment or services in Norway. Norwegian public procurement law is based on the EEA agreement between the EFTA countries and the EU, EU directives and regulations, including the Public Procurement Act[337] and accompanying regulations. These rules emphasizes competition, equal treatment, non-discrimination, transparency, and proportionality in the EEA, and prohibit local preference that would distort competition in the EEA.[338]
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose restrictions on origin of the funds and the manner in which they are invested?	Yes (1) SkatteFUNN R&D Tax Incentive Scheme	(1) SkatteFUNN is Norway's primary tax incentive for research and development. It provides a refundable tax credit (19% of eligible R&D costs) to companies

[335] European Commission, *Rules on international data transfers*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en
[336] Worl Population Review, *Nine Eyes Countries 2025*, https://worldpopulationreview.com/country-rankings/nine-eyes-countries
[337] The Public Procurement Act, Act No. 73 of 17. June 2016
[338] Layer Norway, *Public Procurement in Norway: A Comprehensive Overview,* (April 2025), https://www.lawyernorway.no/articles/public-procurement-in-norway-a-comprehensive-overview

	(2) Innovation Norway Grants	that are tax-liable in Norway and have an approved R&D project.[339] (2) Innovation Norway provides grants and loans for innovation projects, environmental technology, and commercialization efforts. [340]
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?	No	There is no verified evidence of direct foreign interference specifically targeting Norway´s legislative priorities on data and innovation, but there are documented cases of foreign influence attempts in adjacent areas, such as elections and public opinion, which could indirectly affect policy-making. Researchers from the Norwegian Defence Research Establishment (FFI) investigated whether foreign actors attempted to influence Norway´s 2021 parliamentary elections. They did not find direct manipulation of election results, but there were active attempts by foreign actors to influence Norwegian public opinion through disinformation on social media and websites. [341]
Ongoing / Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?	Yes Norwegian Artificial Intelligence Act (Implementation of EU AI Act)	Norway is in the process of incorporating the EU AI Act into national law through a dedicated Norwegian AI Act, scheduled to enter into force in summer 2026. The Act introduces a risk-based regulatory framework for AI systems, with strict obligations for high-risk applications and outright bans on unacceptable-risk

[339] The Norwegian Tax Administration, *Deductions for research and development – SkatteFUNN*, https://www.skatteetaten.no/en/business-and-organisation/tax-for-businesses/tax-return/deductions/research-and-giftsdonations/skattefunn-ordningen/
[340] Innovation Norway*, Funding for innovation projects*, (June 2025), https://en.innovasjonnorge.no/article/funding-for-innovation-projects
[341] H. Lundberg, *Foreign Election Interference*, https://www.andnumbers.com/cases/foreign-election-interference

		systems. The Act aligns Norway with EU standards, ensuring interoperability, and reducing dependency on foreign AI systems. The European regulatory model requires Norwegian businesses to map AI usage and comply with transparency, human oversight, and data quality requirements, fostering local accountability and governance capacity.[342] The European Commission has proposed targeted amendments to the EU AI Act under the "Digital Omnibus" initiative, including delaying key compliance deadlines and simplifying obligations for high-risk AI systems. If Norway implements the AI Act before these adjustments are finalized, it could create a competitive disadvantage compared to countries that postpone or adopt the revised framework, as Norwegian businesses would face stricter requirements earlier than their European peers.[343]

[342] Government of Norway, Paving the way for safe and innovative use of AI in Norway, (March 2025), https://www.regjeringen.no/en/whats-new/gjor-norge-klar-for-trygg-og-innovativ-ki-bruk/id3093081/
[343] JDSUPRA, EU AI Act: Proposed 'Digital Omnibus on AI' Will Impact Businesses' AI Compliance Roadmaps, (November 2025), https://www.jdsupra.com/legalnews/eu-ai-act-proposed-digital-omnibus-on-9937662/

Switzerland

Nicole Beranek Zanon, Härting Rechsanwälte, Zug
Alesch Staehelin, Uto Legal, Zurich

Executive summary

Switzerland understands “digital / technological sovereignty” in a narrow, state-centred way. The core concern is that the Confederation has sufficient control and ability to act in the digital space to perform its public tasks. The broader role of the private sector and society is addressed mainly within the “Digital Switzerland Strategy,” not as independent holders of “sovereignty.”

Since 11 December 2020, the Federal Administration has pursued a hybrid multi-cloud strategy, allowing a mix of internal and external cloud services from several providers. Digital sovereignty is expressly anchored as a strategic objective in the annually updated Digital Switzerland Strategy, in the Foreign Policy Strategy 2024–2027 and in the “Strategie Digitale Bundesverwaltung,” and has triggered numerous parliamentary initiatives. AI is a priority field: based on the report of 12 February 2025, the Federal Council has adopted a regulatory approach with three goals (innovation, fundamental rights including economic freedom, and trust), intends to implement the Council of Europe AI Convention in Swiss law, and favours sector-specific legislation complemented by limited horizontal rules (especially data protection).

In terms of technological autonomy, Switzerland has strong domestic capabilities but relies heavily on foreign infrastructure in practice. ETH Zurich (including the “Apertus” foundation model and the ETH AI Center) and the ETH Domain more broadly provide substantial AI and quantum-technology know-how and compute.

Public AI funding is significant but routed through general research and innovation instruments (ETH Domain, SNSF, Innosuisse, sector programmes), not through a dedicated “sovereign AI” vehicle, and there is no policy objective of full-stack technological self-sufficiency. Most production-grade AI services still run on non-Swiss cloud providers and non-Swiss base models. AI adoption is high, especially in services and finance, but many organisations are cautious in mission-critical areas because of data-protection, outsourcing and sovereignty risks. Legally, there is no general “data ownership” right, no specific text-and-data-mining exception and no “fair use” clause; copyright limitations are exhaustively listed in Arts. 19–27 URG, and there is not yet case law on unlicensed training of AI models. The revised Federal Act on Data Protection (FADP) distinguishes between personal data, sensitive data and “profiling with high risk,” but does not mandate data localisation. Cross-border transfers are governed by Art. 16 FADP (adequate protection or appropriate safeguards); derogations apply only narrowly. Information security for critical infrastructures is regulated in particular by the Federal Act on Information Security (ISA), the Ordinance on the Protection of Critical Infrastructures (VSKI), the National Cyber Strategy and Art. 74a FMG, with potential board liability under Art. 754 CO if risk management (including supplier diversification) is insufficient.

Access to data without consent is only permitted under specific statutes and with strict safeguards. Under the Federal Act on the Surveillance of Postal and Telecommunications Traffic (BÜPF / SPTTA), authorities may obtain data from telecom and cloud providers for serious criminal offences only on the basis of prior judicial authorisation; bulk "collect-all" access and warrant-less access are not allowed. Internationally, Switzerland cooperates via the Budapest Convention and MLATs; foreign authorities cannot directly compel Swiss providers, which prevents direct extraterritorial enforcement such as under the US CLOUD Act. Competition and innovation policy support technological autonomy indirectly: the Cartel Act (KG) and the Federal Act on the Promotion of Research and Innovation (RIPA) form the core framework and are applied by COMCO and the Federal Supreme Court (e.g. BGE 143 II 297, Swisscom) to safeguard infrastructure access and innovation dynamics.

Public procurement law is formally non-discriminatory but allows innovation and sustainability criteria; tax law provides a patent box and an R&D super-deduction under the DBG, linked to R&D conducted in Switzerland and to Swiss-related IP. External influences arise in particular from the EU adequacy decision under data protection law and from lobbying by foreign technology firms during the FADP revision, but without formal loss of legislative autonomy. Forthcoming reforms (a Digital Services Act, an AI regulatory framework and a Federal Act on Cybersecurity) are expected to reinforce Switzerland's regulatory control over key digital technologies.

Defining Technological Sovereignty	
How is technological sovereignty defined in your jurisdiction? What are the most important factors considered? Examples of Factors: ● Political ● Social ● Dependency perspective ● IT Infrastructure ● Legislative perspective (various levels)	The Federal Council defines "***digital (technological) sovereignty***" narrowly and state-centric: it means that the State possesses the necessary ***control*** and ***ability*** to act in the digital space to ensure the performance of state tasks.[344] The focus is therefore on state actors' capability to fulfil constitutional and statutory duties rather than on a broad claim to industry or individual sovereignty.[345] This narrow definition means that the ability of the economy and civil society to exercise control and take action in the digital space is not the focus from a sovereignty perspective, however, this is part of the digital strategy of the Federal Counsel which includes the economy and society in its browder definition.[346]

[344] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022, as of November 26, 2025, p. 5, Chapter 5.1.
[345] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022, as of November 26, 2025, p. 5, Chapter 5.1 f.
[346] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022, as of November 26, 2025, p. 6. Chapter 5.1.

Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?		On 11 December 2020, the Federal Council adopted the Federal Administration's cloud strategy. This strategy pursues a hybrid multi-cloud approach: federal authorities should be able to purchase both internal and external cloud services from multiple providers and combine them with each other.[347]
AI and Technology Sovereignty Policy		
Has your jurisdiction published a national technology sovereignty policy?		Yes, Switzerland has a nationwide “Digital Switzerland Strategy” (Strategie Digitale Schweiz), adopted annually by the Federal Council, which sets the federal framework for digital transformation and explicitly ***includes digital sovereignty*** (as a strategic objective and focus topic.[348]
Does your jurisdiction have a published national AI strategy/policy?		Artificial intelligence is treated as a priority area within the Digital Switzerland Strategy.[349] In addition, on 12 February 2025 the Federal Council was presented the report on regulation of artificial intelligence and, on that basis, decided on a Swiss regulatory approach to AI. This approach is guided by three objectives: strengthening Switzerland as a location for innovation, safeguarding fundamental rights (including economic freedom), and enhancing public trust in AI. To achieve these objectives, the Federal Council defined the following key parameters: - The Council of Europe’s AI Convention will be incorporated into Swiss law. - Any resulting legislative amendments should be as sector-specific as

[347] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z’graggen, 14.12.2022, as of November 26, 2025, p. 15, Chapter 6.1.2.
[348] Monitoringbericht zur Strategie Digitale Schweiz 2023, December 8, 2023, p. 6, Chapter 2.3
[349] Digitale Schweiz - Fokusthema

		possible, while horizontal, cross-sector rules are limited to core areas relevant to fundamental rights, such as data protection. - In addition to legislation, non-binding measures will also be developed to implement the Convention, such as voluntary self-declaration schemes or industry-specific solutions.[350]
Does your jurisdiction have a published AI compute or cloud strategy/policy?		Switzerland has not dedicated on an "AI compute strategy" for the whole economy. However, at federal level there is a clearly defined cloud and AI governance framework for the Confederation[351],, and AI- and cloud-related infrastructure is treated as a priority topic in the nationwide "Digital Switzerland" strategy.[352]
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived operational risks related to technological sovereignty?		Digital sovereignty is a politically salient and strategically anchored topic in Switzerland: The concept of "digital sovereignty" gained prominence in Switzerland's political discourse in 2020 through the report on the needs assessment for a Swiss cloud.[353] It was one of three priorities in the 2022 meetings of the "Beirat Digitale Schweiz". It is explicitly included in the Foreign Policy Strategy 2024–2027 and is one of seven priorities of the 2023 "Strategie Digitale Bundesverwaltung".[354] There are a large number of recent parliamentary initiatives (postulates, motions, interpellations) explicitly on digital sovereignty, cloud, critical digital infrastructures and related issues, which

[350] Bundesamt für Kommunikation, Künstliche Intelligenz, Auslegeordnung und Regulierungsansatz der Schweiz, from 10. March 2025
[351] Swiss Government Cloud
[352] Digitale Schweiz
[353] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022, as of November 26, 2025, p. 2, Chapter 3.
[354] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022, as of November 26, 2025, p. 3, Chapter 3.

		indicates sustained parliamentary activity on the topic.[355]
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?		Yes, in the Public sector, the ETH Zurich released Apertus, a large-scale LLM trained from scratch. [356]
Does your jurisdiction have national AI research centres of excellence?		Yes, the ETH AI Center at ETH Zurich: it is the University's central AI hub and a centre of excellence connecting AI foundation, application and implications research.[357]
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?		Yes. Switzerland has significant domestic quantum computing research, development and early commercialisation capacity, centred on the ETH Domain. ETH Zurich and EPFL host leading laboratories and initiatives in quantum computation and quantum technologies, including participation in major international programmes and operation of advanced experimental quantum processors.
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech stack, funding and adoption.	On the AI tech stack, Switzerland has strong public research and compute (ETH Domain, Swiss National Supercomputing Centre) and first domestic foundation models, but most production-grade AI services used in the market still rely on non-Swiss cloud infrastructure and non-Swiss base models. The Confederation responds mainly with principle-based instruments (FADP, AI Guidelines for the Confederation, Digital Switzerland Strategy, Cloud Strategy / Swiss Government Cloud), not with strict localisation or hard sovereignty mandates. On funding, Switzerland does not run a single, centralised "sovereign AI fund", but channels substantial support through general innovation and research instruments (ETH Domain, SNSF, Innosuisse, sectoral programmes). Public AI funding is material by Swiss standards, but clearly below the large mission-oriented AI programmes of the EU, US or China and is not directed at full stack autonomy. On adoption, Switzerland shows high uptake of AI and especially generative AI in services, finance and industry, with a dense ecosystem of start-ups and	

[355] Digitale Souveränität der Schweiz Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, 14.12.2022, as of November 26, 2025, Annex, p. 25.
[356] Apertus: Ein vollständig offenes, transparentes und mehrsprachiges Sprachmodell | ETH Zürich
[357] Homepage – ETH AI Center | ETH Zurich

	applied research centres. At the same time, many Swiss organisations remain cautious in mission-critical contexts because of data-protection, outsourcing and technological-sovereignty concerns, so overall adoption is broad but risk-sensitive, not “maximalist”. Overall, the Swiss jurisdiction combines: high regulatory and institutional capacity, strong upstream research and compute, reliance on foreign commercial AI infrastructure, and a mature but deliberately conservative adoption pattern driven by data protection, information-security and outsourcing law	
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?		Switzerland does not have a general, cross-sector “data ownership” right or exclusive data right that goes beyond classic intellectual property law.
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and commercialization of innovation?		No, Switzerland does not have a special, explicit text and data mining (TDM) exception comparable to the EU’s DSM Directive, nor a dedicated statutory regime expressly designed to promote TDM-based research and innovation.
Does your jurisdiction have (1) an open, principle-based notion of “fair use” or (2) a closed, listed exceptions-based notion of “fair dealing”? Do those rules favor national players?	(2)	Swiss copyright law (Urheberrechtsgesetz, URG, SR 231.1) is based on the principle that the use of a protected work requires the rightholder’s consent unless they fall under a specifically listed statutory limitation/exception. The main exceptions are laid down in Arts. 19–27 URG (private copying, education, quotation, reporting on current events, etc.). There is no open-ended, US-style “fair use” clause.
Have courts in your jurisdiction issued decisions on the application of “fair dealing” or “fair use” in relation to the use of		In relation to AI models, not yet.

unlicensed data to train AI models (i.e. via screen scraping)		
Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?		Switzerland has no special statutory "data ownership" right. Exclusivity around data arises only through copyright in database structure (Arts. 2 URG), trade and official secrets (Art. 162, 320 f. StGB (Strafgesetzbuch, StGB, SR 311.0); Art. 4 lit. c UWG (Bundesgesetz gegen den unlauteren Wettbewerb, UWG, SR 241)), and personality/data-protection rules – none of which are designed to favour national over foreign players.
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: e) in the public sector? f) in the private sector?	Art. 16 FADP	For the federal administration, the revised Federal Act on Data Protection (Datenschutzgesetz, DSG/FADP, SR 235.1) applies (incl. to cross-border transfers under Art. 16 FADP: transfers abroad are allowed if the destination ensures an adequate level of protection or appropriate safeguards are in place.
What are special classifications of "protected data" (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?	Art. 5 lit. c FADP Art. 16 FADP	Switzerland's Federal Act on Data Protection distinguishes between "personal data" and "sensitive personal data" (besonders schützenswerte Personendaten), and adds "profiling with high risk" as a special risk category, but none of these classifications require that such data be hosted or processed only in Switzerland. Art. 5 lit. c FADP defines sensitive personal data as, in particular, data on religious or political views, health, private life, racial/ethnic origin, genetic and certain biometric data, and data on administrative or criminal prosecutions and sanctions. It also separately defines "profiling with high risk". These categories trigger stricter processing obligations (e.g. transparency, DPIAs, security), but not a

		localization requirement. Cross-border hosting and processing of all types of personal data is governed by Art. 16 FADP: transfers abroad are allowed if the destination ensures an adequate level of protection, or if appropriate safeguards (SCCs, BCRs, etc.) are in place; only in the absence of such conditions do narrow derogations apply.
What are the most notable cross-border data transfer restrictions in your jurisdiction?	Art. 16 FADP	Art. 16 FADP: Personal data may only be disclosed abroad if the destination country ensures an adequate level of data protection. If there is no adequacy, the controller must implement appropriate safeguards (SCC, BCR).
What were the outcomes of the 2-3 most notable regulatory or court decisions in your jurisdiction on the issue of cross-border data transfers?		--
Information Security Laws for critical infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Switzerland has enacted a comprehensive legal framework governing information security for critical infrastructure, primarily anchored in the Swiss Federal Act on Information Security, ISA (Informationssicherheitsgesetz, ISG/ISA; SR 152.3), which entered into force on January 1, 2024. The ISA imposes obligations on federal authorities and entities performing public tasks to implement risk-based security measures, conduct regular vulnerability assessments, and	In addition, the Swiss Ordinance on the Protection of Critical Infrastructures (Verordnung über den Schutz kritischer Infrastrukturen, VSKI) and the National Strategy for the Protection of Switzerland against Cyber Risks (NCS) provide a strategic and regulatory basis for safeguarding essential services such as energy, telecommunications, finance, and healthcare. Operators of critical infrastructure are required to adopt technical and organizational measures aligned with recognized standards (e.g., ISO/IEC 27001) and to report significant cyber incidents to the National Cybersecurity Centre (NCSC) pursuant to art. 74a of the Swiss Federal Act on Telecommunications, TA (Fernmeldegesetz, FMG; SR 784.10).

	ensure continuity of operations. While the ISA directly applies to federal bodies, its principles influence cantonal and private-sector operators of critical infrastructure through sector-specific regulations and public-private partnerships.	
In your jurisdiction, can directors and officers be held accountable for not diversifying critical digital infrastructure or for failing to mitigate the risks associated with supplier-side concentration?		Directors and officers may incur liability under art. 754 of the Swiss Code of Obligations, CO (Obligationenrecht, OR/CO; SR 220) for breaches of their duty of care if they fail to implement adequate risk mitigation strategies, including diversification of suppliers and avoidance of single points of failure in digital infrastructure. Such liability is assessed under the standard of diligence expected from a prudent business leader, as confirmed by Swiss Federal Supreme Court jurisprudence (e.g., BGE 132 III 342).
Lawful Access (Legal access to data without consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?		Swiss law provides for lawful access to data without the consent of affected individuals under specific statutory regimes, subject to strict procedural safeguards. The Swiss Federal Act on the Surveillance of Postal and Telecommunications Traffic, SPTTA (Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF; SR 780.1) authorizes law enforcement authorities to compel telecommunication service providers, including internet and cloud hosting providers, to disclose traffic and subscriber data for the purpose of criminal investigations. Such measures require prior judicial authorization (art. 18 ff. SPTTA) and are limited to cases involving serious offences enumerated in art. 269 ff. of the Swiss Criminal Procedure Act, CPA (Strafprozessordnung, stop/CPA; SR 312.0).

If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a “collect all” regime) under such lawful access regime?		The lawful access regime does not permit bulk data collection or “collect-all” approaches; requests must be specific and proportionate, in compliance with art. 36 of the Swiss Federal Constitution (BV; SR 101) and art. 4 of the Swiss Federal Act on Data Protection, FADP (Datenschutzgesetz, DSG; SR 235.1).
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?		Access without a warrant or judicial oversight is prohibited under Swiss law, ensuring adherence to fundamental rights and the principle of legality.
Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?		Switzerland is a party to international treaties governing cross-border lawful access, notably the Convention on Cybercrime (Budapest Convention) and various Mutual Legal Assistance Treaties (MLATs). These agreements facilitate cooperation while preserving Swiss sovereignty and data protection standards. Foreign authorities cannot directly compel Swiss providers; requests must be channelled through formal MLAT procedures, thereby preventing extraterritorial enforcement such as under the U.S. CLOUD Act.
Competitive Markets for Innovation		
What is the most important statutory regime in your jurisdiction that is intended to promote competitive markets for innovation? What is their most notable impact on promoting		The cornerstone statutory regime is the Swiss **Federal Act on Cartels and other Restraints of Competition (Cartel Act, CA, SR 251)**. Its purpose, as stated in a**rt. 1 CA**, is: *to prevent harmful economic effects of cartels and other restraints of competition and to promote competition in the interest of a liberal market economy.” The CA is complemented by the Swiss **Federal Act on the Promotion of**

technological autonomy?		**Research and Innovation (RIPA, SR 420.1)**, which explicitly aims to strengthen Switzerland's technological autonomy by fostering domestic research capacity and innovation ecosystems. **Notable impact:** ● The CA ensures that dominant undertakings cannot abuse their market power to stifle innovation (see a**rt. 7 CA**). RIPA provides direct funding and incentives for Swiss-based research institutions and companies, thereby reducing dependency on foreign technological solutions.
Have such law(s) been applied by courts and regulatory authorities in your jurisdictions to further technological autonomy?		Yes. The **Competition Commission (COMCO)** and the **Swiss Federal Supreme Court (Bundesgericht)** have applied these laws to safeguard innovation. For example: ● **BGE 143 II 297 (Swisscom case)**: The court confirmed that abuse of dominance in broadband infrastructure could hinder innovation and market entry, thus violating a**rt. 7 CA**. ● COMCO decisions in the ICT sector (e.g., cloud services and telecom) have emphasized that competitive access to infrastructure is essential for technological autonomy. These rulings demonstrate that Swiss authorities interpret competition law not only to protect price competition but also to maintain innovation dynamics
Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable		Switzerland is not part of the "Five Eyes" alliance and is not subject to the US CLOUD Act. However, Switzerland has entered into numerous bilateral and multilateral free trade agreements via EFTA and with the EU.

protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of “Five Eyes”) ?		These agreements generally include provisions on intellectual property and data flows but do not impose material constraints on Swiss technological autonomy. Switzerland also participates in Mutual Legal Assistance Treaties (MLATs), including with the United States, which can affect cross-border data access in criminal investigations. However, these do not directly undermine domestic legislative autonomy on innovation policy.
Does your jurisdiction have any “buy local” federal government procurement rules that apply specifically to advanced technology equipment or services?		Switzerland does not have explicit “Buy Swiss” rules for advanced technology at the federal level. The Swiss Federal Act on Public Procurement (Verordnung über das öffentliche Beschaffungswesen, VöB/PPA, SR 172.056.1) is based on principles of non-discrimination and transparency, aligned with WTO GPA obligations. However, art. 8 PPA allows consideration of sustainability and innovation criteria, which can indirectly favor Swiss suppliers if they meet these standards better than foreign competitors.
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose restrictions on origin of the funds and the manner in which they are invested?		Yes. Switzerland offers significant tax incentives under the Swiss **Federal Act on Tax Reform and AHV Financing (TRAF)** and cantonal regimes, including: ● **Patent box (Art. 24a Bundesgesetz über die direkte Bundessteuer, DBG, SR 642.11)**: Reduced taxation on income from patents developed in Switzerland. ● **R&D Super-Deduction (art. 25a DBG)**: Up to 150% deduction for qualifying R&D expenses. **Restrictions:** These incentives require that R&D activities occur in Switzerland and that intellectual property is linked to Swiss-based development. There are no explicit

		restrictions on the origin of funds, but the substance-over-form principle applies to prevent abuse.
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data and innovation in your jurisdiction?		There have been instances of international pressure during negotiations on data protection and cloud sovereignty. For example: ● During the revision of the Federal Act on Data Protection (FADP, SR 235.1), lobbying from foreign tech companies sought to influence provisions on cross-border data transfers. ● The EU's adequacy decision for Swiss data protection law also exerted indirect pressure, as Switzerland had to align with GDPR standards to maintain data flow with the EU. These influences did not amount to formal interference but demonstrate external impact on legislative priorities.
Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?		Two major reforms are expected to materially affect technological autonomy: ● **Digital Services Act (planned)**: Aims to regulate large online platforms and ensure fair competition in digital markets. ● **AI Regulation Framework (under consultation)**: Will introduce compliance obligations for AI systems developed or deployed in Switzerland, reinforcing domestic control over critical technologies. Additionally, ongoing discussions on **cloud sovereignty** and **cybersecurity law reform** (draft Federal Act on Cybersecurity) will

		strengthen Switzerland’s autonomy in managing technological infrastructure.

United Kingdom

Michael Peeters, Addleshaw Goddard LLP, Leeds
Patricia Shaw, Beyond Reach, London

Executive summary
This report examines the United Kingdom's approach to technological sovereignty and autonomy across key regulatory, policy, trade agreements, and other commercial dimensions. The UK's current policy and legislative framework appears to be emphasising economic growth, innovation leadership, and flexible governance rather than defensive data localisation or explicit sovereignty requirements. The UK (as stands) has no formal definition of 'technological sovereignty' but pursues de facto sovereignty through its National AI Strategy, AI Opportunities Action Plan, the Sovereign AI Unit (established in July 2025), and through significant compute infrastructure investments (£2 billion UK Compute Roadmap) and talent development to ensure the UK is creating its own enablement environment and AI assets. While cloud sovereignty policies remain permissive for the private sector, sensitive government and defence data increasingly stays onshore. This may not be the case for health data held within the NHS. The UK maintains strong research capabilities through the Alan Turing Institute, AI Security Institute, National Quantum Computing Centre, and National Cyber Security Centre, but remains heavily dependent on US hyperscalers and Asian semiconductor supply chains. On the whole there appears to be nothing specific in terms of law reform or anticipated regulatory landscape to enforce or endorse technological autonomy for the UK.

Defining Technological Sovereignty	
How is technological sovereignty defined in your jurisdiction? What are the most important factors considered? Examples of Factors: ● Political ● Social ● Dependency perspective ● IT Infrastructure	No specific definition for technological sovereignty exists in UK policy. However, the Government's focus is clearly on economic growth, UK productivity, and frontier technology leadership rather than concerns about over-dependence on foreign technology. The UK AI Opportunities Action Plan demonstrated this further as it stated UK's ambition to be an AI maker, not an AI taker'. This is further reinforced through the establishment of the UK's Sovereign AI Unit which aims to maximise the UK's stake in frontier AI.

• Legislative perspective (various levels)		
Cloud Sovereignty		
Has your jurisdiction published a national cloud sovereignty policy?	NO except to some extent for UK public sector	Nothing appears to be explicitly mandating that data should be stored in the UK-based cloud infrastructure. The **UK public sector guidance** states: *"There is no government policy which directly prevents departments or services from storing or processing cloud-based data in any specific country, however you need to consider the implications of where you host your data. It is the responsibility of each government department to take risk-based decisions about their use of cloud providers for the storage of government data regardless of the geographic location of the data.* *When making this decision, you should consider the:* ○ *ICO guidance on adequacy* ○ *ICO guidance on data protection and the international transfer of data* ○ *NCSC cloud principles"* https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector Within the UK public sector there are "Crown Hosting" facilities to allow for UK government controlled data centres for secure hosting. In practice, defence and security agencies as well as foreign office type departments will not host outside the UK. Increasingly this is also the case for all central government departments, especially for data considered of value. Furthermore, with UK Data Centres being classified as Critical National Infrastructure under the Network and Information Systems Regulations 2018 (SI

		2018/506) may mean in practice that the requirements to implement appropriate and proportionate technical and organisational measures to manage risks to the security of network and information systems, (with the aim of minimising the impact of incidents to ensure service continuity, and ensuring a level of security appropriate to the risks posed) result in demand-led cloud sovereignty from UK businesses.
AI and Technology Sovereignty Policy		
Has your jurisdiction published a national technology sovereignty policy?	No?	No specific policy, but see e.g. **Industrial Strategy, Digital and Technologies Sector Plan**, which refers to sovereignty – with overarching theme being to make the UK a leader in frontier tech – https://assets.publishing.service.gov.uk/media/6892104df15b237bf6610996/industrial_strategy_digital_and_technologies_sector_plan_accessible.pdf
Does your jurisdiction have a published national AI strategy/policy?	Yes, in name only – as not as yet mature or comprehensive…	Yes – **National AI Strategy:** 1. Invest and plan for the long-term needs of the AI ecosystem to continue our leadership as a science and AI superpower; 2. Support the transition to an AI-enabled economy, capturing the benefits of innovation in the UK, and ensuring AI benefits all sectors and regions; 3. Ensure the UK gets the national and international governance of AI technologies right to encourage innovation, investment, and protect the public and our fundamental values. https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version See also the **AI Opportunities Action Plan:** 1. Invest in the foundations of AI 2. Push hard on cross-economy AI adoption 3. Position the UK to be an AI maker, not an AI taker https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

		The above Action Plan also established the **Sovereign AI Unit**, with the power to partner with the private sector to deliver the clear mandate of maximising the UK's stake in frontier AI https://www.gov.uk/government/collections/sovereign-ai-unit
Does your jurisdiction have a published AI compute or cloud strategy/policy?	Yes for govt – less generally?	The UK Government has a **cloud first policy**; https://www.gov.uk/guidance/government-cloud-first-policy - but this states public cloud should not be used for handling certain categories of secure data. **The AI Compute strategy falls under the "UK Compute Roadmap"**: 1. Invest up to £2 billion to deliver a diverse, joined-up and user centred compute ecosystem, 2. Establish National Supercomputing Centres to curate datasets, build software assets and deliver a skills pipeline to support a broad range of users to access and utilise computing power. 3. Partner with like-minded countries and computing centres to expand access to a broader range of research infrastructure, facilitating collaboration and skills and knowledge exchange. https://www.gov.uk/government/publications/uk-compute-roadmap/uk-compute-roadmap#executive-summary
How lively is the discussion on digital sovereignty is in your country? Is it a salient political issue? Are some of your clients taking active steps to mitigate perceived		As mentioned above, the Government's tech/AI strategy appears to be focused economic growth and prosperity. In contrast, a lot of the commentary – e.g. examples below – highlights the risks in overdependency and geo-political instability. However, both the third-party commentary and that of the Government recognizes that a balanced

operational risks related to technological sovereignty?		approach is required, to both develop the UK's domestic capability and continue to leverage relationships with international partners. https://www.newstatesman.com/spotlight/tech-regulation/public-sector-tech/2025/06/digital-sovereignty-should-sit-at-the-core-of-the-uks-ai-strategy https://www.cityam.com/government-urged-to-prioritise-uk-tech-amid-us-investment-surge/ https://www.civo.com/digital-sovereignty-revolution-report-2025
Technological Autonomy Maturity		
Does your jurisdiction have domestically developed foundational AI models? Public or private sector?	Yes	Yes – e.g. Stability AI (private sector)
Does your jurisdiction have national AI research centres of excellence?	Yes	The **Alan Turing Institute** – UK's national institute for data science and AI – https://www.turing.ac.uk/ The **EPSRC also funds and supports nine AI research hubs** focused on particular projects – https://www.ukri.org/news/100m-boost-in-ai-research-will-propel-transformative-innovations/
Does your jurisdiction have domestic quantum computing research, development and/or commercialization capacity?	Yes	The **National Quantum Computing Centre (NQCC)** is the UK's national lab for quantum computing, focused on translating UK quantum research into innovation. The NQCC is funded by the government (EPSRC).
Briefly describe your jurisdiction's current level of technological autonomy and maturity as regards AI tech	The UK relies heavily on: ○ the US and Asia in relation to hardware (e.g. semi-conductors) and the largest AI model providers (e.g. OpenAI). ○ US tech vendors and hyperscalers for a large proportion of hosting and critical software.	

stack, funding and adoption.		
Data Ownership/Exclusive Data Rights		
Does your jurisdiction have special laws or provisions providing database ownership rights or exclusive data rights (beyond basic copyright laws)?	Yes	The Copyright and Rights in Databases Regulations 1997[358]. This gives a wide definition of "database" as "a collection of independent works, data or other materials which a) are arranged in a systematic or methodical way, and b) are individually accessible by electronic and other means". The works which make up the Database may or may not be protected, separately to the Database as a whole. The Database right applies where a "substantial investment" has been made in gathering and organising the content of the database. Investment means "any investment, whether of financial, human or technical resources" and substantial means "substantial in terms of quantity or quality or a combination of both". This specifically means an investment in arranging the content, as opposed to creating the content itself. It is infringed when data is extracted or re-utilised without permission. The Database right expires at the end of the period of fifteen years from the end of the calendar year in which the making of the database was completed or first made available to the public.
Does your jurisdiction have a special statutory regime to treat text and data mining (TDM) or to otherwise promote research and	Partially	Section 29A Copyright, Designs and Patents Act 1988[359] provides an exception for TDM, for ***non-commercial purposes***. This exception applies so long as access to the copyright material is lawful and there is acknowledgement of the author (where appropriate).

[358] https://www.legislation.gov.uk/uksi/1997/3032
[359] https://www.legislation.gov.uk/ukpga/1988/48/section/29A

commercialization of innovation?		Lawful access includes, for example, access via a paid subscription for content which is behind a paywall, or access to content which is freely available on the internet.
Does your jurisdiction have (1) an open, principle-based notion of "fair use" or (2) a closed, listed exceptions-based notion of "fair dealing"? Do those rules favor national players?	Fair dealing system	We have a fair dealing system which provides various exceptions to copyright infringement[360]. The exceptions were introduced to distinguish the issue of fair dealing from the issue of whether there had been use of a work constituting infringement, as these issues were often conflated[361]. These exceptions include: ● non-commercial research and private study; ● criticism, review and reporting current events; ● teaching; ● helping disabled people; ● time-shifting; ● parody, caricature and pastiche. At a surface level, this favours national players, however due to the requirement for copying to take place in the UK (to establish copyright infringement under the CDPA 1988), the application of these rules is somewhat limited.
Have courts in your jurisdiction issued decisions on the application of "fair dealing" or "fair use" in relation to the use of unlicensed data to train	No	The only UK case in which primary infringement and the application of fair dealing exceptions has been argued to date was Getty Images v Stability AI [2024] EWHC 2863 (Ch). However, the primary infringement case was dropped and so we have not yet had a finding on this matter.

[360] https://www.gov.uk/guidance/exceptions-to-copyright

[361] Copinger and Skone James on Copyright 19th Edition, Part 1, Chapter 8, Part 6, Section A: https://uk.practicallaw.thomsonreuters.com/Document/ICEF679300B8711E88611E4F4ADBEA029/View/FullText.html?ppcid=e6fd5b90f9644cf39ae823dc3e82668c&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Category)&nortId=IF4BCBB200B8711E8AAC0F3BAE73D7CCB&navigationPath=%2FDocument%2FICECD1F400B8711E88611E4F4ADBEA029%2FView%2FFullText.html%3Fppcid%3D301f725176b34d0283cc8274ffeea3fb%26originationContext%3Ddocumenttoc%26transitionType%3DCategoryPageItem%26contextData%3D(sc.Category)%26nortId%3DIF4C609F00B8711E8AAC0F3BAE73D7CCB%26comp%3Dbooks%26navId%3DB138524F6AC134D6EDECD9BC4EEBB7D7&comp=books&navId=1A4414465C7EC7DBE202B96345CF8802

AI models (i.e. via screen scraping)		
Are there any other special exclusivity rights provisions (data ownership in a strict sense) in your jurisdiction? Do those rules favor national players?	No	N/A
Data Protection (Personal Information)		
What are the most notable data sovereignty/localization provisions applicable in your jurisdiction: a) in the public sector? b) in the private sector?		The **Data (Use and Access) Act 2025 (DUAA 2025)**represents the most significant UK data protection reform since the UK GDPR. However, it too does not include any specific provisions concerning data sovereignty or localization. Key provisions do include: (1) A new 'data protection test' for international transfers replacing the 'essentially equivalent' standard with 'not materially lower'—providing greater transfer flexibility; (2) New 'recognised legitimate interests' lawful basis removing balancing test requirements for certain processing; (3) Enhanced ICO enforcement powers and PECR fines aligned to GDPR levels; (4) Mandatory internal complaint-handling mechanisms. The European Commission has indicated it will approve the UK's adequacy status under this new regime (July 2025 press statement). References: gov.uk/government/collections/data-use-and-access-act-2025; /
What are special classifications of “protected data” (e.g. classified, top secret) that must be hosted and processed only within your jurisdiction? What are the legal basis of such classifications?		The Data (Use and Access) Act 2025 has introduced new powers for the Secretary of State to add or remove special categories of data to the list in Article 9 of the UK GDPR via regulation. Whilst nothing explicit has been provided for concerning hosting and processing within the UK, the DUAA 2025 has not sought to make international transfers harder by the introduction of the data protection test.

What are the most notable cross-border data transfer restrictions in your jurisdiction?		There appears to be less notable cross-border data transfer restrictions and more cross-border data enablement. For example, the UK-US Data Bridge being an extension of the EU-US Data Privacy Framework, facilitating cross border transfers to certified UK organisations. Furthermore, the EU has just endorsed an adequacy decision concerning the protection of personal data for the purposes of cross-boarder EU-UK data transfers which is now set to expire on 27th December 2031.
Information Security Laws for critical infrastructure		
Does your jurisdiction have information security laws for critical infrastructure (state owned, or private sector) which require any special considerations?	Yes	Network and Information Systems Regulations 2018 (NIS) – set to be reformed by the Cyber Security and Resilience Bill (https://www.gov.uk/government/collections/cyber-security-and-resilience-bill) The regulation applies to Critical National Infrastructure which is defined as: *"Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), where the loss or compromise of which could result in:* ● *Major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or* ● *The Significant impact on national security, national defence, or the functioning of the state."* Data centres were expressly added in September 2024 and this includes both the physical data centres and the cloud operators that use them to supply services.

		The regulatory provisions are intended to: ● help anticipate and minimise chances of major issues arising from critical incidents, ● through a dedicated CNI data infrastructure team of senior government officials: ○ monitor and anticipate potential threats; ○ provide prioritized access to security agencies (including the National Cyber Security Centre (NCSC)); and ○ co-ordinate access to emergency services should an incident occur. ● Restrict transfer of ownership to certain categories of overseas owner.
Lawful Access (Legal access to data without consent)		
Does your jurisdiction have law(s) that provide law enforcement authorities with the right to obtain access to personal data held by telecommunication service providers, cloud hosting service providers or enterprises without the consent of the affected individuals and, if so, do such laws permit lawful access by foreign authorities?	Yes - RIPA	Under the Investigatory Powers Act 2016, limited UK authorities may access or intercept data held about an individual by a telecoms provider with a warrant issued by the Secretary of State. Such a warrant will only be issued for national security purposes, to prevent or detect serious crime, or in the interests of the economic well-being of the UK so far as those interests are also relevant to national security. “Communications data” (data about the communications and not the content itself) may be obtained by a broader category of authorities for broader purposes, and this can be authorised by the Investigatory Powers Commissioner. Access for limited purposes can also be authorised by designated senior officers within the relevant authority. A foreign authority may make a request for access in relation to an individual based in the UK at the time of interception if a warrant has been issued in relation to such individual.

		Foreign authorities may also make requests to telecoms providers under an international agreement, or initiate interception through mutual assistance agreements (see below).
If so, are bulk data transfers authorized (i.e. transfers not only about specifically identified individuals, but also classes of individuals, such as a "collect all" regime) under such lawful access regime?		Bulk interception warrants can only be issued in relation to communications sent or received by individuals outside the British Islands. Only the security and intelligence agencies may apply for such warrants, and the Secretary of State must personally authorise the interception.
Do such regimes provide for the possibility of such lawful access without a warrant or judicial oversight?		Interceptions can take place without a warrant: ● With consent of the sender or recipient ● For administrative or enforcement purposes ● In prisons, psychiatric hospitals or other detention facilities In addition, data may be intercepted by or on behalf of a telecoms provider, without a warrant, on request by a foreign authority under an international agreement to which the UK is a party, provided that the relevant individual is (believed to be) outside the UK.
Has your jurisdiction entered in treaties or cooperation agreements that treat lawful access to data? If so, might these agreements further constrain data rights under local law in your jurisdiction?	Yes	The UK is a party to various mutual legal assistance (MLAT) agreements, and the Crime (International Co-operation) Act 2003 provides statutory powers for seeking and providing such assistance in relation to criminal matters. The Investigatory Powers Act allows for warrants to be issued for interception requests to give effect to such mutual assistance agreements. Applications can also be made by foreign authorities for these purposes.

		In addition, the UK-US Data Access Agreement US law enforcement to directly request data held by telecommunications providers in the UK for the exclusive purpose of preventing, detecting, investigating and prosecuting serious crimes such as terrorism and child sexual abuse and exploitation.
Procurement Rules and Trade Commitments		
Has your jurisdiction entered into any free trade agreements that place constraints or grant notable protections as regards technological autonomy (e.g. under US Cloud Act, an MLAT or as part of "Five Eyes") ?		The UK has a number of free trade agreements in place. For example, the UK-EU Trade and Cooperation Agreement. Article 234 covers protection of technological measures, requiring parties to provide legal protection against the circumvention of technological measures (being technology that stops people from using copyrighted material without permission, e.g., password protection/encryption). There is also the Agreement on Government Procurement, however this does not consider defence / technology.
Does your jurisdiction have any "buy local" federal government procurement rules that apply specifically to advanced technology equipment or services?	Not as such	No, there are no specific "buy local" procurement rules relating to tech. However, the following are worth noting: ● The Procurement Act 2023 (the "Act") has a national security exemption set out at Schedule 2, Paragraph 25 gives contracting authorities discretion to procure national security contracts outside of the Act. ● Schedule 5, Paragraph 5 of the Act also features a direct award justification on the basis of a supplier having exclusive rights to supply goods/services, which is quite regularly used to award contracts to a particular supplier without running a competitive procurement process (however, this may not be strictly relevant to the question). ● The Government's Security Classifications Policy restricts the dissemination of sensitive materials to "UK eyes only", which could restrict matters to being in the UK only.

		• Procurement Policy Note 11/20 applies to below threshold contracts and allows you to reserve the procurement by supplier location (meaning only suppliers in a certain area can bid, e.g., UK-wide, by county, etc). However, this is not tech-related specifically and will not apply to above-threshold procurements.
Tax		
Does your jurisdiction provide tax incentives or other similar incentives to further technological autonomy? Does these incentives impose restrictions on origin of the funds and the manner in which they are invested?	Yes (1) Research & Development Tax Credits; (2) Patent Box regime.	Although there is not a specific tax relief targeted only at technological autonomy, there are certain tax reliefs which are likely to be relevant. (1) The UK operates a research and development (R&D) tax credit regime, whereby an enhanced proportion of cost expended on innovative R&D is available as a credit for the relevant company, either resulting in a reduction of taxable profits or an actual cash credit receivable from the UK tax authority, HMRC. Broadly R&D only applies to work carried out in the UK, unless there are exceptional reasons why it cannot be carried out in the UK. (2) A patent box regime where profits attributable to UK registered patents can be subject to a lower corporation tax rate of 10% (compared to the main rate of 25%). (3) There are other indirect regimes which could be useful, such as the EMI share option scheme, offering tax efficient share incentives to employees in UK growth companies and the SEIS and EIS schemes which offer reliefs to investors who invest into qualifying UK growth companies.
Data and Innovation Policy Autonomy		
Have there been any notable examples of foreign interference with national legislative priorities related to data		There does not appear to be explicit notable examples of foreign interference. However the UK recognised the changing nature of the role of foreign interference in light of emerging technologies. According to the UK Government's

and innovation in your jurisdiction?		Final Statement of Strategic Priorities for online safety published on 2 July 2025, the UK Government is concerned about the use of AI tools (such as generative AI used with or without being in conjunction with social media platforms) to facilitate 'coordinated inauthentic behaviour at scale' … 'to manipulate the information environment'. It notably sees that this is a potential space for foreign interference to take place undermining democratic processes. It envisages that illegal foreign interference would be included in Ofcom's illegal content Code of Practice which is also to cover 'state-sponsored disinformation, aimed at subverting the UK's democratic, political and legal processes. The statement call for urgent guidance on how platforms should 'mitigate and tackle illegal foreign interference' and not only be able to identify when an emerging threat is taking place but then have the guidance and potentially resources to respond to such emerging threat(s). https://www.gov.uk/government/publications/statement-of-strategic-priorities-for-online-safety/final-statement-of-strategic-priorities-for-online-safety Ofcom's Illegal Content Codes of Practice under the Online Safety Act 2023 (OSA 2023) address foreign interference as a priority offence. This offence is included in Schedule 7 of OSA 2023, which lists priority offences requiring service providers to take action to prevent their platforms from being used to facilitate such criminal activities. Foreign interference is defined under section 13 of the National Security Act 2023 (NSA 2023). In short, this covers conduct carried out for, on behalf of, or with the intent to benefit a foreign power, which interferes with UK rights, discredits democratic institutions, manipulates participation in democratic processes, or undermines the safety or interests of the UK (having a so-called interference effect under Section 14 of the NSA 2023).

		Illegal Content Codes of Practice provide detailed guidance on these measures, which are tailored to the size and risk profile of the service provider. Compliance with these codes offers a safe harbour for service providers.
Anticipated Law Reform		
Is there any (anticipated) material law reform in your jurisdiction that is likely to have a materials impact on issues related to technological autonomy?		The UK has signaled that it might produce a homegrown **AI Regulation** Bill. As stands, the UK maintains a 'pro-innovation' sectoral approach rather than horizontal EU AI Act-style legislation, though this remains under review. It is likely that in any case, new law would be targeted at the use of frontier models whether and to what degree this will be used to provide technological autonomy through limited use of third country frontier models, is as yet uncertain. The Cyber Security and Resilience Bill is currently embarking on its parliamentary legislative journey The UK has introduced new legislation concerning product liability and safety with the enactment of the **Product Regulation and Metrology Act 2025**. This Act establishes a broad framework enabling the government to pass secondary legislation aimed at addressing modern safety issues. As the scale and scope of the secondary legislation has not as yet been clarified, this provides scope for the UK to bring about a product liability regime to include software in the definition of product so that it includes harm caused by emerging technologies in line with the EU. Furthermore, while the Act itself does not directly amend the existing product liability provisions under the Consumer Protection Act 1987, it provides the government with powers to introduce further regulations in priority areas, such as the sale of unsafe products through online marketplaces and addressing hazards posed by emerging technologies. The effect of this legislation may impose non-tariff trade barriers to companies of third countries preventing them (or making it very difficult

		for them to) access to the UK market for certain types of technology. To the extent that technological autonomy can be limited through market dynamics the UK's Digital Markets, Competition and Consumers Act 2024 defines a position of 'strategic significance' in relation to a digital activity (rather than wider technological activity) under section 6. An undertaking is considered to have such a position if one or more of the following conditions are met: (a) the undertaking has achieved a position of significant size or scale in respect of the digital activity; (b) a significant number of other undertakings use the digital activity as carried out by the undertaking in conducting their business; (c) the undertaking's position in respect of the digital activity enables it to extend its market power to other activities; or (d) the undertaking's position in respect of the digital activity allows it to determine or substantially influence how other undertakings conduct themselves, either in relation to the digital activity or otherwise. Apart from the above and anticipation of secondary legislation, there appears to be nothing specific in terms of law reform to enforce or endorse technological autonomy.

Methodology and Contributors

Written at a time when the rules-based international order is under threat, phase one of this report is deliberately grounded in a legal/policy analysis. This report canvasses perspectives from a variety of "middle power" jurisdictions (Argentina, Canada, France, Germany, Italy, Norway, Switzerland and the United Kingdom) that are wrestling with issues of technological sovereignty.

Under the direction of Charles Morgan, a group of lawyers, comprised primarily of members of ITechLaw and the Human Technology Foundation, first aligned upon a template for the legal/policy survey that forms the basis of the individual country reports, executive summaries of which are included in Annex A to this report. Once the individual country reports were completed, the Canadian team prepared a draft of the main body of the report, based on common themes that emerged from the eight country reports. The draft of the main report was then circulated for comments from the entire set of contributors listed below resulting in the current document.

This "phase one" report identifies a series of vulnerabilities and risks to technological sovereignty from a legal/policy perspective. "Phase two" of the analysis, set out in a distinct report, examines the practical tradeoffs faced by businesses, where technological decisions routinely involve tensions between competing objectives: resilience versus cost, performance versus security, control versus simplicity. It proposes concrete, actionable tools to inform strategic decision-making to help address such vulnerabilities and risks.

Name	Company	Location
Bertrand Cassar	La Poste	Paris, France
Emmanuelle Mignon	August Debouzy	Paris, France
Mathilde Lécaillon	Lawways Avocats	Paris, France
Gilles Rouvier	Lawways Avocats	Paris, France
Grimaud Valat	Duclos, Thorne, Mollet-Viéville & Associés (DTMV)	Paris, France
Alexander Tribess	GreenGate Partners Rechtsanwaltsgesellschaft GmbH	Hamburg, Germany
Dr. Philip Kempermann	Heuking	Dusseldorf, Germany
Licia Garotti	Pedersoli Gattai	Milan, Italy
Marco Galli	Pedersoli Gattai	Milan, Italy
Kristian Foss	Bull & Co	Oslo, Norway
Michael Peeters	Addleshaw Goddard LLP	Leeds, UK
Patricia Shaw	Beyond Reach	London, UK
Nicole Beranek Zanon	Härting Rechsanwälte	Zug, Switzerland
Alesch Staehelin	Uto Legal	Zurich, Switzerland
Francis Langlois	McCarthy Tétrault	Montreal, Canada
Charles Morgan	McCarthy Tétrault	Montreal, Canada
Diego Fernandez	Marval, O'Farrell & Mairal	Buenos Aires, Argentina
Éric Salobir	Human Technology Foundation	Paris, France

HUMAN TECHNOLOGY
FOUNDATION

ITECHLAW®
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION