Insight Paper: AI Sovereignty

October 2025
GSMA member confidential

This document was requested by GSMA Policy Group Global in March 2025. It has been developed with members of the GSMA AI for Impact policy and regulatory group. The purpose of this paper is to provide an overview of the current policy conversation on AI sovereignty and key considerations for MNOs, as it is increasingly referenced as a priority for countries and regions, and there are a variety of perspectives and approaches.

Overview

Artificial intelligence (AI) sovereignty refers to a state's ability to develop, deploy and govern AI technologies autonomously within its borders, in alignment with its own legal, ethical, cultural and political values. AI sovereignty encompasses control over the data, algorithms, infrastructure and regulatory frameworks that underpin AI systems. In this context, 'sovereign AI' describes an AI system created, operated and controlled entirely in one jurisdiction.

In recent years, some countries have started treating AI as a non-negotiable strategic national project, recognising that it will be a determinant of economic success and political influence. A government's wish to work on AI sovereignty can be to realise one or several priorities such as national ambitions to become a leader in AI, economic gains through more efficient products and services, or considerations of national security, strategic autonomy and the risks of over-reliance on foreign technology providers.

Attitudes to AI sovereignty have renewed interest in cloud and data sovereignty. Regarding data sovereignty, there is no internationally agreed definition, but it usually refers to the idea that data is subject to the laws and governance structures of the sovereign state in which it is collected, generated or processed. It is sometimes associated with the term data localisation, which refers to regulatory requirements to store sensitive, personal or all data within a specific geographical boundary, such as a country's borders, unless an exemption is approved. The fact that data is integral to the training and deployment of AI models has focused new attention on data sovereignty as a concept. This raises questions regarding national security, economic competitiveness and privacy and trust, especially when data is stored or processed across borders. Poorly designed or implemented data sovereignty measures can risk inhibiting digital innovation and growth.

Closely related is the concept of cloud sovereignty, or the ability to use cloud computing services in compliance with national regulations, ensuring that data stored in the cloud is protected from foreign access and especially from laws with extraterritorial jurisdiction. This has led to increased interest in 'sovereign cloud' solutions, whereby only local entities and partnerships manage and access cloud infrastructure within a country's borders under strict security controls. Cloud sovereignty is seen as important for protecting sensitive data and for ensuring regulatory compliance.

Different approaches and opinions on sovereignty remain. Many countries will not be able to develop and deploy AI in complete digital isolation. Not all countries have access to the significant computational resources and curated datasets needed to train large language models or general-purpose models. The limited global pool of AI talent is another key restriction, making it difficult for some nations to train or retain expertise. Given the significant costs involved in the independent development of the full AI stack, most countries may find a collaborative approach to be faster, more efficient, and ultimately more practical. In this sense, sovereign AI can be seen as a continuum rather than a checklist. Countries will need to assess the inherent strengths, weaknesses and gaps in their domestic AI ecosystems and identify the strategic partnerships and collaborations required to realise their AI ambitions.

This paper gives an overview of the global policy landscape on AI sovereignty, highlighting some of the key events in recent years and the main considerations by policymakers. It also addresses the critical role telecoms operators can play in helping countries achieve their sovereignty ambitions.

The GSMA has not published any material on AI sovereignty in particular; however, the industry's existing global policy position on cross-border data flows is related, as data sovereignty measures linked to AI sovereignty can restrict cross-border data flows. The GSMA supports the free flow of data across borders, emphasising that it drives economic growth, innovation and digital transformation. It discourages unjustified data localisation mandates and promotes interoperable frameworks that balance data flows with the protection of personal data and privacy, referencing the APEC Cross-Border Privacy Rules (CBPRs) and the Global Cross-Border Privacy Rules (CBPR) system. The GSMA encourages regulatory harmonisation to reduce fragmentation and to facilitate trusted cross-border data movement supported by clear legal safeguards.

Global policy landscape

The term 'AI sovereignty' has been popularised in recent years and used frequently by countries and the private sector, in particular since the start of 2025. However, policies and ambitions around sovereignty in the digital sphere are not new. Regarding data sovereignty, the California Consumer Privacy Act (CCPA) of 2020, the European Union's General Data Protection Regulation (GDPR) of 2016, and the Japan Act on the Protection of Personal Information, most recently updated in 2022, all aim to protect and retain control of their citizens' personal data.

Recently, China and the United States have moved to consolidate their AI dominance (e.g., through trade policy, public investment or attracting/retaining talent), while other countries are exploring different approaches to assert their sovereignty and gain a foothold.

Since 2017, China has introduced strict rules for algorithm governance, data localisation and export controls on AI chips and data. Chinese legislation on AI also mandates complete government oversight and control of end-to-end AI.

The United States, under the Biden and Trump administrations, has focused on domestic control over AI development and maintaining global AI leadership. This includes the largest

public-private partnership to date on AI, Project Stargate, which coordinated $500 billion of investment in domestic AI infrastructure.

India passed its Digital Personal Data Protection Act in 2023, introducing principles of data sovereignty, including localisation for sensitive personal data. Subsequently, the IndiaAI Mission, launched in 2024, emphasises compute infrastructure, talent development, indigenous datasets and particularly strategic autonomy, with India positioning itself as an alternative to the US and China.

In 2025, the European Commission published the AI Continent Action Plan, outlining the EU's strategy to become a global leader in AI and aiming to boost the EU's AI innovation capabilities. The plan includes elements designed to promote and invest in EU technology capacity in areas relevant to telecom providers, for example the promotion of EU cloud. The plan cements the bloc's 'regulate first' reputation.

National or regional LLMs, such as LATAM-GPT or SwissLLM, both announced in 2025, are funded by national governments and built on public infrastructure, providing an open-source LLM tailored to the region's linguistic, cultural, and historical contexts and aiming to provide more accurate and specific results, enabling better use in key sectors such as healthcare and education.

Rather than focus on the national level, some regions are looking to consolidate efforts. At the Global AI Summit on Africa in 2025, 54 countries and the African Union signed the Africa Declaration on Artificial Intelligence, seeking to leverage the potential of AI, ensuring all aspects of the AI ecosystem and the related benefits are available within Africa. This built on African Union's Data Policy Framework and Continental AI Strategy, and subsequently several African countries, including Kenya, Nigeria and South Africa have drafted or updated AI strategies that emphasise sovereign infrastructure and regional data ecosystems.

The private sector is working with states to increase AI sovereignty. In 2019, NVIDIA launched its AI Nations initiative, aiming "to help … countries spanning every region of the globe to build sovereign AI capabilities, including ecosystem enablement and workforce development." In May 2025, OpenAI introduced 'OpenAI for Countries', modelled on the US Stargate project, to establish public-private partnerships in other countries to increase national AI capacity through formalised infrastructure collaboration.

Mobile operator contributions to AI sovereignty

MNOs provide last-mile connectivity between AI applications, end users, and compute nodes and resources, perfectly positioning them to work with the public sector to scale up the domestic AI ecosystem, particularly in areas such as distributed inference, edge intelligence and the synergy between 5G and AI.

Some MNOs are already engaging with sovereignty-related initiatives. The following examples illustrate some of the ways MNOs can support government ambitions as trusted partners.

- Telus will invest US$50.6 billion over five years into sovereign AI data centers and other infrastructure, supporting the new Canadian Sovereign AI Compute Strategy.
- Telenor AI Factory announced a strategic partnership with Norwegian AI firm Bineric to strengthen the development of sovereign AI technology.
- Swisscom's new Swiss AI Platform enables firms to build and operate AI applications while meeting the "highest sovereignty requirements."
- The UAE Sovereign Launchpad, developed by e& and Amazon Web Services (AWS), and endorsed by the UAE Cyber Security Council, is a new product to accelerate cloud and AI adoption for government and regulated sectors.
- Singtel has collaborated with IMDA and other governmental agencies to launch a sovereign AI cloud service, RE:AI, spurring AI adoption and innovation while reducing dependency on global cloud platforms.
- Deutsche Telekom and NVIDIA have agreed to build Europe's first sovereign industrial AI cloud by 2026, endorsed by German Chancellor Friedrich Merz as an "important step."
- Vodafone and Fastweb launched FastwebAI Suite, a platform of GenAI-based services and tools dedicated to business and government in Italy.
- Jio Platforms and Bharti Airtel are contributing to India's IndiaAI Mission and Digital India initiatives, developing edge AI and sovereign cloud infrastructure with local compliance.

Global policy considerations

There are a variety of motivations for countries to move toward models of increased AI sovereignty, as well as limitations; essentially, that total AI sovereignty is difficult to achieve for most states, and therefore disadvantageous to pursue. In recent years, many governments, regions and institutions have re-examined their approach to AI sovereignty, often as part of broader AI strategies. Although the points outlined below do not apply universally, they reflect key considerations for policymakers.

Driving forces

Future competitiveness

Some countries are concerned about over-reliance on global tech giants or other states when it comes to AI and want to prevent 'digital colonialism', whereby technologies, infrastructure and domestic data are used in a manner that benefits external entities disproportionately. By fostering research and development and supporting local AI ecosystems, states aim to retain and invest in the most valuable parts of the AI value chain. This may involve protection for domestic innovation through intellectual property (IP) rights.

Local culture and context

There are concerns that global AI models and AI ecosystems made up of foreign companies will not accurately reflect the local culture and context, resulting in sub-optimal outcomes for local users. For example, AI systems trained and developed with local data, in a local language and with local knowledge can provide better results in fields such as education and healthcare.

Policymakers may look to exercise IP rights over cultural, linguistic and heritage content, to formalise how it is used and managed with respect to AI. Concerns have been raised in national and international fora that, without local control, AI risks reinforcing foreign biases and making decisions that are misaligned with local needs.

Security and strategic autonomy
Some policymakers perceive national security risks associated with foreign access or control of aspects of the AI ecosystem, raising concerns around espionage, surveillance, economic security and resilience. Changing geopolitical and trade relationships have encouraged countries to think about the effect of possible export controls and sanctions, restrictions on access to the AI ecosystem and dependence on foreign AI and cloud providers. This has led to calls for supply-chain diversification and locally controlled infrastructure to handle the most sensitive workloads.

Efficiency
Developing localised infrastructure, including data centres and cloud infrastructure, can provide faster AI inference and reduce dependence on foreign providers. Edge computing delivers significant advantages by processing data closer to where it is generated rather than relying solely on centralised cloud infrastructure. This approach reduces latency, improves reliability and optimises bandwidth, which improves the performance of real-time applications such as autonomous vehicles and industrial automation. By distributing compute power, edge computing also supports the scalability of massive IoT deployments. Beyond performance, investing in localised infrastructure for AI strengthens security resilience and improves environmental efficiency. Sensitive data can be processed locally, reducing exposure to cyber threats and supporting compliance with national regulations.

Data embassies
States may consider data embassies as a resilience mechanism and precaution against natural disasters, cyberattacks or conflict, whilst allowing for data localisation. Data embassies, sites located outside a sovereign state geographically but under the control and jurisdiction of that state, are being used as a means to retain full control of data, while physically storing it outside the geographical jurisdiction.

Data privacy and protection
Consumers may have concerns about the use of their personal data to design and train AI. AI developed and deployed in line with a country's laws and regulations, and in keeping with local values of governance, might be seen as more trustworthy. This could motivate governments to increase sovereignty measures related to AI development and use, in order to reestablish data privacy norms and compliance with local laws, encouraging public trust and legitimacy needed for increased uptake of AI.

Concerns and restrictions

Infrastructure and skills gaps

The vast majority of countries will not be able to develop and deploy AI entirely in isolation, lacking sufficient expertise, compute capacity and access to data, or even reliable source of electricity to power AI. Developing sovereign cloud infrastructure, chips and AI models from scratch can be prohibitively expensive and duplicative. Hence, countries need to review and assess their own AI ecosystem, identifying strengths, weaknesses, over-dependencies and vulnerabilities. This assessment can guide the development of strategic partnerships and targeted programs to strengthen domestic capabilities and advance AI sovereignty. In many ways, this mirrors longstanding discussions on supply-chain resilience.

Fragmentation and inefficiency

There are concerns that strict sovereignty measures can lead to a fractured global AI landscape, reducing interoperability and stifling international collaboration. A lack of interoperability could undermine efforts to create shared global frameworks for responsible AI, making international governance harder. Localisation efforts could also restrict access to global AI models and datasets and reduce movement of talent, which could result in slower innovation and limited R&D.

Cross-border data flows

The free flow of data would be restricted by overly prescriptive AI sovereignty and related data-sovereignty requirements. This could present a future challenge to individuals, businesses and policymakers in using data to support evidence-based decision making, to develop LLMs and other AI-enabled applications, or where R&D and innovation require collaboration and transfer of data outside one state.

Key considerations for MNOs

Widespread and growing attention on AI sovereignty opens up potential opportunities for MNOs as trusted partners to government, given their domestic presence, data, infrastructure and relationships. However, there are concerns around lack of clarity or overly strict models of sovereignty that could hinder MNOs' business operations and interests.

Opportunities

Localised solutions

Because mobile infrastructure is located within state borders, MNOs can offer cloud computing and data storage more locally than hyperscalers do via regional hubs. Telcos can expand their data centers with computing infrastructure to support sovereign AI models. This domestic presence can be seen as an advantage by governments interested in sovereignty, as edge computing is increasingly favoured to speed up AI inference and improve energy efficiency and security. Some countries have advocated for strict sovereignty requirements that would require sovereign AI service providers to be immune to third-country laws.

Security
MNOs operate essential national infrastructure. Developing or hosting AI domestically strengthens security, ensures greater control over sensitive data, reduces exposure to external constraints, and builds resilience in the face of global supply-chain disruptions. Increased AI sovereignty, therefore, provides a foundation for safer, more reliable and more autonomous operations, as well as enabling edge computing and the associated benefits.

Trust and Public Perception
Consumers and governments increasingly expect MNOs to safeguard user data and operate transparently. The sector is already heavily regulated in this regard, and so sovereignty measures allow operators to use their existing relationship to consumers and the public sector to strengthen trust and show alignment with national interests, which can be crucial for public-private partnerships.

Concerns

Taxonomy
Inconsistent and overlapping use of terms such as AI sovereignty, digital sovereignty, data localisation, data residency and data sovereignty across legal, regulatory and technological contexts is causing confusion. The lack of standardised definitions complicates compliance, implementation and cooperation.

Cross-border data flows
A patchwork of data localisation requirements and mechanisms spurred by different countries' sovereign AI goals would limit cross-border data flows and therefore MNOs' ability to operate across borders and access global AI models and data resources, hindering competitiveness. New mandates for local data storage, processing and infrastructure deployment would increase operational and compliance costs.

Lack of regulatory clarity and cohesion
Sovereignty is increasingly referenced as a priority in national and regional AI strategies. However, in many instances, this is not followed up with concrete action or policy, affecting MNOs' ability to plan for the future. Governments are also taking different stances on sovereignty, increasing the likelihood that MNOs operating in different markets will have to comply with different and potentially conflicting regulatory models.

Looking forward

The GSMA recognises that emerging policies linked to AI sovereignty will impact mobile operators differently, depending on the markets they are active in and the nature of their business. With this in mind, the GSMA encourages members to stay abreast of policy developments on sovereignty in their markets and to reach out to GSMA regional teams for support where needed.

Operators have an opportunity to contribute to national and regional AI sovereignty goals by leveraging their local knowledge, consumer trust, ecosystem relationships, datasets and local infrastructure. In markets where sovereignty is a priority, operators may wish to engage proactively with governments to explore areas where they can provide solutions.

The GSMA will continue to monitor the global policy landscape on AI sovereignty and update members on relevant trends or influential actions. The GSMA will reflect on, and where necessary, refresh the mobile industry position on cross-border data flows. The GSMA's Capacity Building programmes can equip policymakers with an understanding of policy issues such as AI sovereignty, based on real-world experience and academic insight.

Annex I – Glossary

There are no internationally agreed-upon definitions for many of the terms related to data sovereignty, however, below is a list of commonly used definitions, to accompany this document.

AI sovereignty – The control and autonomy a sovereign state has over the development, deployment, and governance of all aspects of the AI ecosystem within its borders.[1] Sometimes referred to as 'AI nationalism'.

Cloud sovereignty – A cloud-computing environment that is owned, deployed, governed and managed within a sovereign state. It is made up of some aspects of digital, data and operational sovereignty.[2]

Data embassy – A data centre, located outside of a sovereign state's territory, but storing that state's data and under the control and subject to the governance of that state. They can be useful in situations where localised servers are compromised by cyberattacks or natural disasters, or can provide additional compute power for periods of heightened data traffic.[3][4][5]

Data localisation – An explicit requirement that data be stored and/or processed within the domestic territory.[6] It is worth noting that some taxonomies or jurisdictions use the terms 'data localisation' and 'data sovereignty' interchangeably.

Data residency – Data that is being stored in a different sovereign state from the one where it was generated.[7]

Data sovereignty – The concept that data is subject to the laws and governance structures of the sovereign state in which it is collected, generated or processed.[8]

Digital or technology sovereignty – A sovereign state's ability to shape the digital transformation in a self-determined manner with regard to hardware, software, services and competencies. With regard to digital technologies and applications, this means being able to decide independently to what extent one enters into or avoids dependence on providers and partners.[9][10]

---

[1] What Is Sovereign AI? NVIDIA, February 2024

[2] The journey to cloud sovereignty – Assessing cloud potential to drive transformation and build trust, Capgemini Research Institute, 2022

[3] https://e-estonia.com/wp-content/uploads/factsheet_data_embassy.pdf

[4] https://www.dsci.in/dsci-blog/content/data-embassies-legal-and-technological-implications-india

[5] https://www.dsci.in/dsci-blog/content/data-embassies-legal-and-technological-implications-india

[6] A PRELIMINARY MAPPING OF DATA LOCALISATION MEASURES, OECD TRADE POLICY PAPER June 2022 n°262

[7] What is data sovereignty? IBM Think, June 2024

[8] THE NATURE, EVOLUTION AND POTENTIAL IMPLICATIONS OF DATA LOCALISATION MEASURES, OECD TRADE POLICY PAPER November 2023 n°278

[9] Digital sovereignty – easy and simple, DT, April 2025

[10] What is digital sovereignty and how are countries approaching it? World Economic Forum, January 2025

Indigenous data sovereignty – The right of individuals, peoples or communities to govern the collection, ownership, and application of their own data,[11] including in some cases the right to process personal data based on applicable data protection laws in local customs, traditions and contexts.

Operational sovereignty – The ability of an organisation or sovereign state to independently control and maintain critical infrastructure and operations, ensuring that core systems function under national or organisational control.[12]

[11] Permanent Forum on Indigenous Issues 23rd Session, UN Economic and Social Council, April 2024
[12] Digital sovereignty – easy and simple, DT, April 2025