

By Amanda Kraley, Izabela Kantor, and Rodrigo Gutiérrez

Introduction to independent research with POLITICO

At G42, we envision a future where artificial intelligence (AI) becomes an indispensable utility, as integral to our daily lives as electricity. This vision is embodied in our concept of the Intelligence Grid, designed to integrate AI into every facet of people and planet advancement, delivering knowledge, assistance, and capabilities on demand. The Intelligence Grid relies on a scalable infrastructure, ensuring that AI services are always accessible, reliable, and secure.

Realizing the full potential of the Intelligence Grid requires a comprehensive approach to data governance and sovereignty. As AI shapes economic competitiveness and national security, the frameworks that govern data become critical. Diverse legal, cultural, and political contexts influence how data is managed, localized, and protected, affecting AI infrastructure development and operation. Our collaboration with POLITICO's Research and Analysis Division on the independent research report, "Sovereign AI Ecosystems: Navigating Global AI Infrastructure and Data Governance," was to better understand the articulation of these issues and their potential solutions.

This report explores the relationship between data sovereignty and AI infrastructure, providing a strategic overview of the current landscape and future trends. It examines how different jurisdictions approach data governance and highlights the challenges and opportunities that arise from varied legal and cultural contexts. Understanding these dynamics is crucial for stakeholders navigating global digital transformation. The localization and international flow of data are intertwined with governance frameworks, making it essential to develop symbiotic policies that support the sustainable growth of equitable AI technologies.

For G42, the Intelligence Grid is not just a technological endeavor but a strategic vision for the future of AI. By harmonizing AI advancements with robust data sovereignty, we aim to create a secure, interconnected digital ecosystem that benefits everyone. Our collaboration with POLITICO's Research and Analysis Division in producing this research report underscores our commitment to encouraging a global dialogue on AI infrastructure and data governance.

Central to our Intelligence Grid concept is the establishment of resilient data Centers and compute capabilities, designed to handle the immense data processing and storage demands of modern AI applications. Complementing this infrastructure is our focus on developing sovereign cloud solutions, ensuring that data remains within national borders or multilateral data corridors and complies with all relevant regulations, reinforcing data sovereignty.

Advanced network connectivity is another essential component of the Intelligence Grid, ensuring seamless communication and data transfer between AI systems. This connectivity supports uninterrupted AI services, making them as reliable and ubiquitous as electricity. By integrating these components, the Intelligence Grid enables the efficient and secure deployment of AI capabilities across various sectors.

The insights from this independent research report can assist in informing policies and strategies that aim to ensure AI serves as a responsible, transformative, secure and reliable utility. Together, we can contribute to a future where AI, powered by the Intelligence Grid, drives innovation and growth while safeguarding the sovereignty and security of data globally.

Faheem Ahamed

Group Chief Marketing and
Communications Officer, G42

Understanding the strategic development of artificial intelligence (AI) infrastructure and robust data governance has never been more important. This report explores these pressing issues, mapping the global legislative landscape and analyzing the influence of data governance frameworks on the physical infrastructure of AI, highlighting the role of data centers and supercomputers. By examining the global influence of major regulatory frameworks on development of AI infrastructure, the report provides valuable insights on how nations are navigating the complex regulatory environment, ensuring compliance while fostering innovation. Understanding and strategically managing these elements is crucial for nations to drive economic stability and technological advancement in an increasingly interconnected digital world.

In brief

Global regulations like the GDPR, CSL, and CLOUD Act significantly influence AI development and data sovereignty, shaping data center localization, operational compliance, and international data flows.

There is a continued trend towards developing national data sovereignty frameworks, especially outside of North America and Europe. Countries across Asia, South America, and Africa are increasingly adopting localized data governance policies to ensure data remains within their borders to promote national security and economic growth.

Data sovereignty frameworks can be categorized into themes of privacy, protectionism, efficiency, and hybrid approaches. Understanding these themes helps clarify different governance priorities and strategies.

Despite the complexity of varying data sovereignty laws, global investment in AI infrastructure remains robust, with investments striving to keep pace with the growing demand for data storage and processing.

Companies are increasingly adapting their AI strategies to comply with regional data governance laws, leading to the construction of more localized data centers and the development of innovative solutions to manage data within legal frameworks.

The harmonization of data governance standards across regions presents both challenges and opportunities, encouraging international cooperation to establish common principles such as safety, security, and trust.

Section I

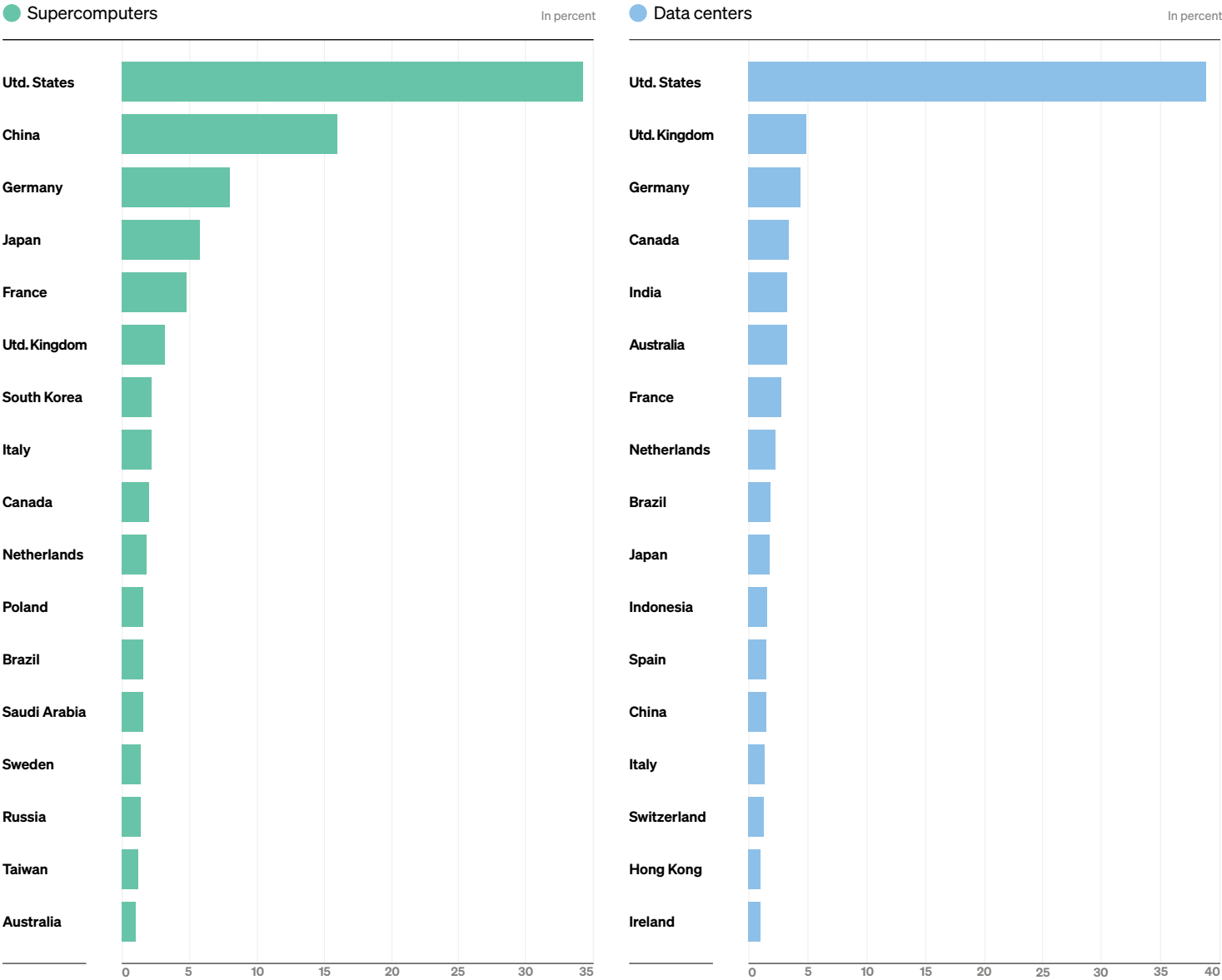
Data governance and AI infrastructure legislative landscape mapping

Rapidly evolving digital technologies present both opportunities and challenges for data governance and sovereignty. As AI becomes crucial to economic competitiveness and national security, the strategic importance of AI infrastructure such as supercomputers and data centers has dramatically increased. By 2023, global investment in AI reached almost **\$843 billion**, with projections only indicating continued growth as countries continue to increase their investments.

Effective data governance frameworks become increasingly critical as the demand for data, data storage, and the computational power to process it accelerates with AI advancements. This surge pertains not just to volume but also data complexity, necessitating sophisticated and scalable data management solutions to harness the full potential of AI technologies, along with strategies that address these shifting paradigms. Understanding the relationships between these regulations and the physical infrastructure supporting AI is essential for leveraging its benefits while ensuring compliance and safeguarding data sovereignty.

Leading supercomputer and data center locations

Share of global supercomputers and data centers per country, in percent



Source: POLITICO analysis based on Top 500 (2024) and Data Center Map (2024) data



From data sovereignty to AI sovereignty

In the contemporary digital landscape, the concept of sovereignty has evolved beyond traditional territorial boundaries to encompass the digital domain. Data sovereignty refers **to the idea that data is** subject to the laws and governance structures within the nation where it is collected, stored, or processed. Building on this foundation, AI sovereignty extends these principles to the realm of artificial intelligence, asserting that the development, deployment, and regulation of AI technologies should also align with national laws and priorities.

A closer look at the connection between AI sovereignty and data sovereignty reveals how regulatory frameworks define and enforce these concepts. The three most globally influential include the European Union's General Data Protection Regulation (GDPR), China's Cybersecurity Law (CSL), and the United States' Clarifying Lawful Overseas Use of Data (CLOUD) Act. While these three are the most globally recognized models and emblematic of three distinctive approaches to sovereignty, they only represent a portion of the world. Expanding the scope of analysis and assessing how a wider range of nations approach data and AI sovereignty can provide a more comprehensive picture of global trends and best practices.

The effects of digital borders

As data flows across borders, understanding and navigating the complex landscape is essential for ensuring compliance, security, and strategic advantages. Data sovereignty is especially relevant for discussions around AI, which relies on vast amounts of data for training, validation, and deployment. The effectiveness of AI systems hinges on access to diverse and comprehensive datasets, which are often sourced globally.

In this context, the intricate web of data sovereignty regulations can significantly impact AI development in a couple of key ways: cross-border data flows and compliance requirements that necessitate operational changes.

First, data localization laws affect dataflow across borders. This, in turn, limits or expands the availability of datasets that could be used for AI training. Too much of a limitation can inhibit the development of robust and accurate AI models, which require large and diverse datasets to perform effectively. However, high standards around privacy and intellectual property might encourage trust and cooperation among data providers, potentially leading to increased sharing of high-quality datasets under compliant frameworks.

Second, compliance with varying data sovereignty laws can introduce operational complexity as companies may need to establish multiple data centers in different jurisdictions to comply with local laws, among other requirements, that have the potential to increase costs. Data sovereignty laws often emphasize the importance of data security and privacy, imposing variable requirements on how data is stored, processed, and transferred.

The success of the AI economy hinges on effective data governance. A well-defined legal framework is crucial for ensuring that data is managed responsibly, securely, and in compliance with both national and international regulations. This governance is essential for maintaining public trust, protecting privacy, and ensuring compliance with national and international laws. In an era where data functions as a critical asset, strong governance practices are essential to mitigate risks such as data breaches and regulatory non-compliance, which could otherwise stifle the development of AI technologies and their ability to operate efficiently. Without effective data governance, the risks of data breaches, non-compliance, and loss of public trust can significantly hinder the growth and development of AI technologies. How specific countries approach data sovereignty greatly affects how they can participate in the global expansion of AI technologies, underscoring the importance of data governance with global reach.

What is a data center?

A data center is a facility used to house computer systems and its associated components. It typically includes redundant power supplies, data communications connections, environmental controls, and various security devices. Data centers are critical for storing, managing, and disseminating data, serving as the backbone for most modern computing applications, including cloud services, web hosting, and enterprise operations. Supercomputers, often housed within data centers, provide the high-performance computing power necessary for advanced data processing and computational tasks.

In the context of AI, data centers are vital for providing the massive computational power and storage capacity required for training AI models, processing large datasets, and running AI applications. They host the hardware and software infrastructure necessary for AI operations, such as high-performance servers, graphics processing units (GPUs), and specialized AI accelerators. These facilities ensure the efficient and secure processing of data, which is crucial for developing and deploying AI technologies.

What is a supercomputer?

A supercomputer is a highly advanced computing machine capable of processing complex and large-scale calculations at extremely high speeds. It is composed of thousands of processors working in parallel, making it ideal for tasks that require substantial computational power, such as climate modeling, quantum mechanics simulations, and genomic research.

Supercomputers are integral to AI development, especially for tasks like deep learning and neural network training, which involve processing vast amounts of data and performing numerous calculations simultaneously. By leveraging the power of supercomputers, AI researchers can significantly accelerate the training process of complex models, enabling more sophisticated and accurate AI applications. These supercomputers are often integrated within data centers, utilizing their robust infrastructure for optimal performance and scalability in AI operations.

From the digital to the material world

The world’s major data governance frameworks serve as the primary points of comparison throughout this report. These frameworks highlight the critical role different governance models play in shaping the global data environment and analyze the ways they impact the development of data centers.

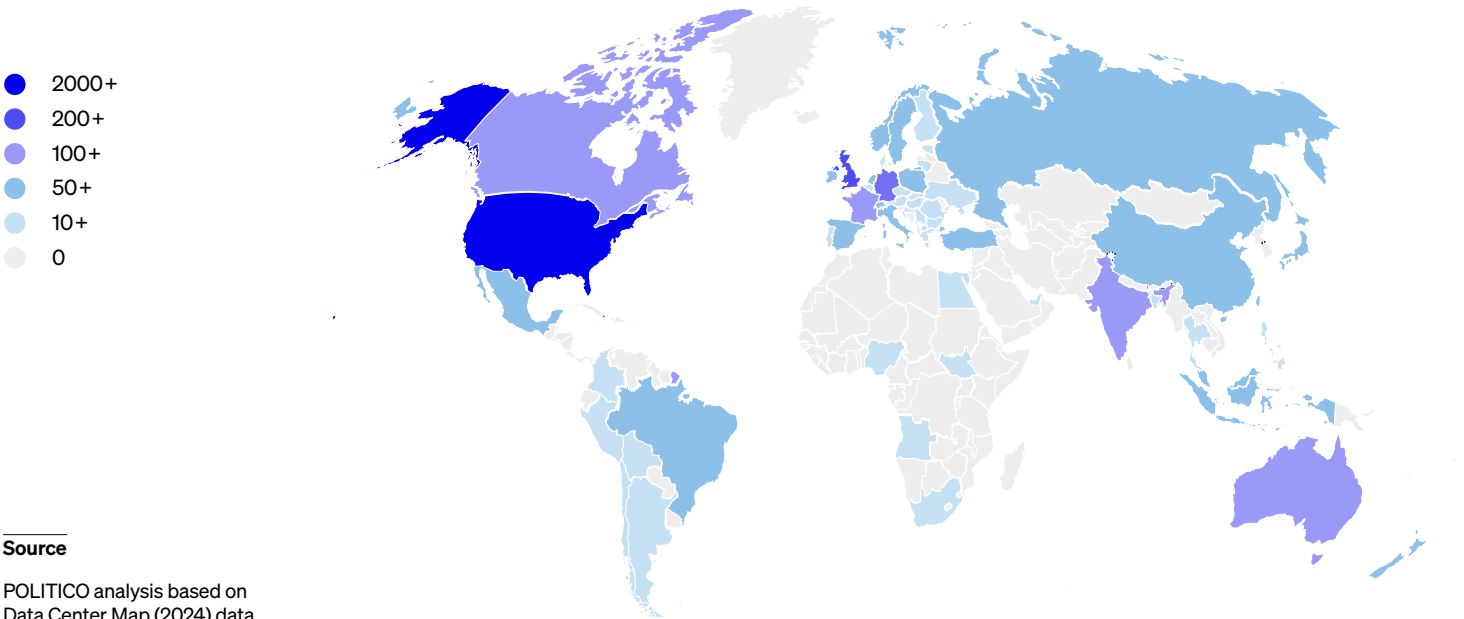
The development of data centers and supercomputers represents the physical infrastructural connection to AI infrastructure. This link highlights how regulatory frameworks translate into tangible assets that support the global AI economy. Examining the global distribution of data centers reveals both the geographical concentration and dispersion of data infrastructure, providing valuable insights into the key hubs of data activity around the world. Identifying these hubs allows for a better understanding of the strategic locations where data is stored, processed, and utilized. These indicators are useful for demonstrating which data governance frameworks have the most reach, highlighting regions with significant investments in data infrastructure.

The concentration of data centers and supercomputers offers valuable insights into the impact and effectiveness of various data governance policies on the global AI economy. This analysis assists in identifying frameworks that attract data-related investments effectively and promote robust AI ecosystems. While not all data centers can accommodate the specialized hardware and requirements for AI, they remain a crucial part of the digital infrastructure ecosystem, facilitating data storage, management, and general processing that underpin many AI-related activities.

Breaking down the numbers

Leading supercomputer and data center locations

Share of global data centers per country



Data centers

Data center distribution reveals insights into the underlying infrastructure supporting AI development and the broader AI economy. High concentrations of data centers indicate regions with robust AI capabilities, driven by substantial investments in computational resources and data storage facilities. These hotspots are where data governance policies are especially influential, guiding research to understand the most impactful regulations and frameworks that shape AI infrastructure and ensure data sovereignty.

Looking at the numbers, the United States boasts the largest network of data centers in North America and globally. The US owes this standing to its historical advantage, with a substantial technological infrastructure and the presence of major tech companies. Europe is also home to several key data center hubs. As of 2024, the United Kingdom, Germany, and France respectively rank first, second, and third, complemented by high digital adoption rates and stringent data protection regulations like GDPR.

In Asia, India, Japan, and China are leading the way, with India boasting the highest number of data centers, followed by Japan and China. Singapore and Hong Kong, known for their strategic locations and advanced infrastructure, also play vital roles in the region. In the Middle East, Saudi Arabia and the UAE are emerging as regional leaders in data center growth. Their significant investments in digital infrastructure and strategic planning have positioned them as key players in the region.

South America's data center market is led by Brazil, housing the most data centers, supported by its large economy and growing internet penetration. Chile and Argentina also have notable data center presences, reflecting regional digital growth. In Africa, South Africa stands out with the highest number of data centers, serving as the continent's key digital hub. Kenya and Nigeria are emerging as important markets, fueled by increasing internet usage and investments in digital infrastructure. Oceania's data center landscape is dominated by Australia, benefiting from its robust economy and a high rate of digital adoption.

Several key factors drive the global distribution of data centers: robust economies and high digital adoption rates are major contributors, along with effective regulatory environments that shape where data centers are established. Advanced technological and physical infrastructure is equally crucial, as is market demand for cloud services and digital technologies. Overall, the global distribution of data centers underscores the critical role of data infrastructure in fueling economic growth, technological advancement, and regulatory compliance in today's interconnected world.

Supercomputers

Comparing the rankings of supercomputers and data centers reveals significant insights into their geographical distribution and concentration. Both prominently feature technologically advanced nations such as the United States, Germany, and Japan, reflecting their strong infrastructure and investment in technology. However, the patterns of distribution between supercomputers and data centers vary considerably, shedding light on different technological priorities and strategies across countries.

The United States leads both categories, but its dominance is more pronounced in the realm of data centers, where it holds a substantially larger share. This suggests that data centers are more heavily concentrated in fewer countries, with the United States being the primary hub. It also reflects a historical technical advantage. In contrast, the distribution of supercomputers is more evenly spread among several countries. China ranks second in the number of supercomputers, indicating a significant presence in high-performance computing that is not as evident in the data center rankings.

Beyond the leading nations, the spread of supercomputers is more balanced. Countries such as Japan and France, which rank high in the supercomputer list, show that high-performance computing resources are distributed across a diverse range of regions. This contrasts with the data center rankings, where there is a steep drop after the United States, and fewer countries hold substantial shares. This sharp decline highlights a higher concentration of data centers in a small number of countries.

The presence of unique entries in each list illustrates different regional focuses. Countries like South Korea, Saudi Arabia, and Poland are noteworthy for supercomputer rankings but are absent from the top data center rankings. This suggests that these countries have made targeted investments in high-performance computing for specific sectors or research needs. Conversely, countries like India and Indonesia appear in the data center rankings, reflecting their growing digital economies and increasing reliance on cloud services, without a corresponding emphasis on supercomputing infrastructure.

Although both supercomputers and data centers are distributed globally, supercomputers show a more geographically diverse presence, with numerous countries making significant investments, reflecting a more balanced global spread. On the other hand, data centers are more concentrated in fewer countries, particularly the United States, pointing to different technological investment strategies and regional focuses across the world.









Section II

Different approaches to AI sovereignty

The analysis of the most globally significant data sovereignty frameworks focuses on countries across continents with substantial data infrastructure. These nations were selected for their robust data and AI capabilities, particularly in terms of data centers and supercomputers. By identifying the top 2-3 countries within each region, the study highlights areas that hold significant influence in shaping data governance and its global impact.

Global legislation overview

A table listing the countries with the most data centers and supercomputers per region, along with their key data sovereignty regulations








Country	Law / legislation	Key provision
Africa		
 South Africa	Protection of Personal Information Act (POPIA)	Allows transfers to countries with adequate protection; permits transfers with safeguards or consent.
 Nigeria	Nigeria Data Protection Regulation (NDPR)	Requires protection measures for transfers; mandates compliance and consent for cross-border transfers.
 Kenya	Data Protection Act	Restricts transfers to countries with adequate protection; requires safeguards and user consent.
Asia		
 China	Cybersecurity Law	Requires data localization for critical information infrastructure; allows transfers with security assessments and user consent.
 India	Proposed Personal Data Protection Bill	Mandates data localization for sensitive data; allows transfers with adequacy decisions, clauses, or consent.
 Japan	Act on the Protection of Personal Information (APPI)	Requires adequate protection for transferred data; allows transfers with adequacy decisions, clauses, or consent.
Europe		
 European Union	General Data Protection Regulation (GDPR)	Restricts transfers to countries with adequate protection; mandates strong safeguards for data transfers, such as standard contractual clauses or binding corporate rules.
 United Kingdom	Data Protection Act 2018	Aligns with GDPR; enforces strict data protection measures and ensures adequacy in data transfers.

Source
POLITICO analysis



Global legislation overview

A table listing the countries with the most data centers and supercomputers per region, along with their key data sovereignty regulations

Country	Law /legislation	Key provision
Middle East		
 Saudi Arabia	Personal Data Protection Law (PDPL)	Requires data localization; restricts data transfers unless necessary measures are taken to ensure data protection.
 UAE	UAE Personal Data Protection Law	Enforces strict data protection measures; allows data transfers with adequate protection and safeguards
North America		
 United States	Clarifying Lawful Overseas Use of Sata (CLOUD) Act	Allows law enforcement access to overseas data
 Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	Requires reasonable steps for protection during transfers; transparency on cross-border flows.
Oceania		
 Australia	Privacy Act 1988	Requires steps to ensure foreign recipients protect data; mandates consent or protection measures.
South America		
 Brazil	General Data Protection Law (LGPD)	Requires consent for transfers; allows transfers to countries with adequate protection or via specific mechanisms.
 Argentina	Personal Data Protection Act	Allows transfers to countries with adequate protection; requires protection measures for transfers.

Source
POLITICO analysis

Data sovereignty regimes are often analyzed based on their geographic and policy landscapes, with predominant frameworks emerging from Europe, the United States, and China. While these three dominate discussions due to their global reach, it is crucial to widen the scope of analysis to include other countries. Each country has unique traits that contribute to shaping data and AI sovereignty strategies.

There is a continued trend towards data sovereignty, including an increase in the development of national frameworks, especially outside of North America and Europe. Examining the broader thematic similarities among these frameworks allows for better contextualization of their different priorities and a deeper understanding of the nuances of each governance approach globally. This understanding is essential for identifying the key elements of data governance that drive policy decisions and their impact on AI infrastructure.

In addition to the EU’s GDPR, the US’s CLOUD Act, and China’s CSL, this analysis provides a deep dive into representative frameworks from major global regions. This detailed examination of global frameworks offers valuable insights into the practical implications of these policies on AI infrastructure and data governance.

Section II – Deep Dive

General Data Protection Regulation

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The **General Data Protection Regulation** (GDPR), often referred to as the strongest privacy and security law in the world, is a comprehensive legislative framework in application in the EU since 2018, that governs the way that personal data of individuals in the EU may be processed and transferred.

The regulation defines individuals' fundamental rights within a digital context to give them more control over their personal data, as well as obligations for data processors, methods for ensuring compliance, and sanctions against those in breach of these rules. To this end, the GDPR enshrines seven core protection principles related to the processing of personal data. These can be identified as follows:

Core protection principles under Article 5 GDPR

Lawfulness, fairness, and transparency

Personal data must be processed in a lawful, fair, and transparent manner to data subjects

Purpose limitation

Data must only be processed for the legitimate purposes that were explicitly specified to data subjects when collected

Data minimization

Data collection and processing should be limited to only what is necessary for the purposes specified

Accuracy

Data must be accurate and kept up to date; inaccurate data must be erased or rectified without delay

Storage limitation

Data that may personally identify data subjects may only be stored for the purposes specified and not longer than necessary

Integrity and confidentiality

Data must be processed in a manner that ensures appropriate security, integrity, and confidentiality (e.g. via encryption)

Accountability

Data controllers are responsible for demonstrating compliance with all principles

While it was adopted in the EU, the GDPR's jurisdictional reach is extraterritorial (Article 3). Compliance is mandated from any entity, irrespective of geographic location, that processes the personal data of EU citizens and residents. In other words, the regulation applies to all organizations—including those that are not based in the EU—if they handle data belonging to EU data subjects.

Given its strict data handling and processing rules, the GDPR significantly impacts several sectors, including AI. AI developers must ensure that their infrastructure complies with key requirements such as:

- ① guaranteeing data minimization and transparency in data processing, as well as compliance with all other core protection principles (Article 5);
- ② obtaining explicit consent from data subjects (Articles 6-7) or the consent of parents for children under 16 years of age (Article 8);
- ③ avoiding the processing of personal data that reveals sensitive information like racial or ethnic origin, religious beliefs, political opinions, genetic information, or sexual orientation, as this is strictly prohibited except in certain circumstances (Article 9);
- ④ incorporating data protection by design and by default, ensuring that such protection is integrated into AI system architecture from the outset (Article 25);
- ⑤ maintaining a record of data processing activities (Article 30);
- ⑥ notifying supervisory authorities of any personal data breaches and communicating to data subjects any such breaches without undue delay (Articles 33-34);
- ⑦ conducting data protection impact assessments (DPIAs) for high-risk processing activities (Article 35);
- ⑧ designating data protection officers (DPOs) to inform and advise data controllers and processors, monitor compliance, and cooperate with supervisory authorities (Articles 37-39);

Implications for global data access and compliance

The GDPR significantly influences the international flow of data, as it imposes strict rules on the transfer of data outside of the EU and greater European Economic Area (EEA). It specifically mandates that personal data can only be transferred to non-EU countries that ensure an adequate level of data protection (Article 44). This requirement is typically satisfied through **adequacy decisions** (Article 45) adopted by the European Commission, which certifies that non-EU countries offer data protection comparable to that within the EU.

However, for countries without an adequacy decision, organizations may rely on alternative mechanisms (Article 46), such as **Standard Contractual Clauses** (SCCs) and **Binding Corporate Rules** (BCRs). SCCs are voluntary, pre-approved legal contracts that provide assurances regarding the protection of personal data transferred to countries outside of the EEA. BCRs, on the other hand, are internal data protection policies adopted and adhered to by multinational companies established in the EU to ensure data protection across their global operations outside of the Union.

These mechanisms have profound implications for businesses and international markets. Through the enforcement of these stringent rules, the GDPR indirectly compels non-EU companies to enhance their data protection practices to maintain access to EU markets. This regulatory export creates a spillover, also said to be the **“Brussels Effect”**, influencing legal systems beyond the EU and thereby driving up global data protection standards altogether.

In terms of data used in the context of AI, AI systems must support data subject rights such as access, rectification, erasure of personal data, restriction of processing, notification, data portability, and objection (Articles 15-21). This strict regulatory landscape significantly impacts both the architectural design and operational processes of AI infrastructure. Emphasis on privacy by design encourages embedding data protection measures at every stage of the AI lifecycle, from initial design to deployment. This can include privacy-preserving techniques such as anonymization, pseudonymization, and secure data storage methods, which influences the types of data AI systems can use and their processing methods.

As the GDPR dictates rigorous data handling practices and protection measures, AI systems must incorporate robust mechanisms to ensure data integrity and confidentiality, such as encryption and secure access controls. Ongoing compliance efforts include regular audits, impact assessments, and continuous monitoring of data processing activities to detect and mitigate potential privacy risks. These requirements compel AI developers and operators to establish comprehensive data governance frameworks that can adapt to evolving regulatory demands and ensure ongoing adherence to GDPR standards, including extensive documentation and reporting mechanisms to demonstrate compliance.

The cost implications of GDPR compliance for AI operations are therefore significant and involve both direct and indirect expenses. Direct costs include investments in technological upgrades for encryption, anonymization, pseudonymization, and secure data storage. Organizations may also need to invest in developing or acquiring tools for data subject access requests (DSARs) and consent management systems. Indirect costs include ongoing compliance measures, such as conducting regular DPIAs, hiring or training DPOs, and maintaining robust compliance frameworks for continuous monitoring and auditing.

While the cost of compliance is high, the cost of non-compliance can be even higher, including substantial fines and penalties (Articles 83-84) and potential reputational damage. Compliance with the GDPR is incentivized as it promotes best practices in data governance and privacy, enhances data security, and fosters consumer trust. This, in turn, can provide a competitive advantage and facilitate access to the privacy-conscious European market.

Section II – Deep Dive

The United States' Clarifying Lawful Overseas use of Data (CLOUD) Act

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, adopted by the United States in 2018, is a legislative framework that addresses the complexities of cross-border data access and law enforcement. It provides mechanisms for U.S. authorities to obtain data stored abroad and allows foreign governments to request data stored in the U.S. under certain conditions.

The act attempts to streamline the process for accessing electronic communications and data across borders, addressing the challenges posed by the global nature of data storage and the internet.

Core provisions: global access

Bilateral agreements

The U.S. may enter into bilateral agreements with other countries, allowing for mutual access to data for law enforcement purposes under specified conditions. (Title II, Section 2523)

Data requests and compliance

U.S. law enforcement can compel U.S.-based technology companies to provide data stored on servers, regardless of the data's physical location. Similarly, foreign governments with an executive agreement with the U.S. can request data directly from U.S. companies, bypassing traditional diplomatic channels. (Title I, Section 103; Title II, Section 2523)

Privacy and civil liberties safeguards

Bilateral agreements must meet several criteria, such as prohibiting targeting individuals based solely on their political views. (Title II, Section 2523(b)(1)(B)); Ensuring data requests are specific and based on credible evidence. (Title II, Section 2523(b)(1)(A))

Judicial review and transparency

Requests for data access are subject to judicial review to ensure they are lawful and appropriate. Additionally, transparency measures are in place to inform the public about the number and nature of data requests made and complied with. (Title I, Section 103(a)(3); Title I, Section 103(f))

Implications for global data access and compliance

Technology companies operating in multiple jurisdictions must navigate the requirements of the CLOUD Act while also adhering to local data protection laws. This often involves implementing robust compliance frameworks and developing processes to handle cross-border data requests efficiently (Title I, Section 103). Organizations may need to invest in legal and technical resources to ensure they can respond to data requests promptly while maintaining compliance with varying international regulations. This includes understanding the specific requirements of each bilateral agreement and ensuring data protection measures are in place to safeguard user privacy (Title II, Section 2523).

The CLOUD Act has significant implications for international data flows and law enforcement cooperation. By providing a legal framework for cross-border data access, it helps address the jurisdictional challenges that arise when data relevant to investigations is stored in different countries (Title I, Section 103).

However, the act also raises concerns about potential conflicts with other nations' data protection laws, such as the EU's GDPR. While the CLOUD Act seeks to balance law enforcement needs with privacy protections, its extraterritorial reach can create legal and operational challenges for multinational companies (Title II, Section 2523).

The CLOUD Act represents an influential approach towards addressing cross-border data access. By establishing a legal framework for international cooperation, it aims to enhance law enforcement capabilities while addressing privacy and civil liberties. However, the act also underscores the challenge of balancing security needs with the protection of individual rights, particularly in the context of global data flows and international data protection standards. As the digital landscape continues to evolve, the CLOUD Act will likely play a crucial role in shaping the future of international data access and cooperation.

Section II – Deep Dive

Cybersecurity law of the People's Republic of China

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The Cybersecurity Law of the People's Republic of China (CSL), enacted in 2017, is a comprehensive legislative framework that governs cybersecurity practices and the protection of personal data within China. The CSL aims to safeguard national security, protect public interests, and secure the rights and interests of citizens in the digital realm.

The law outlines various requirements and obligations for network operators, critical information infrastructure operators, and other entities involved in handling personal data and maintaining cybersecurity.

Core provisions: cybersecurity and data protection

Network Operators' Responsibilities

Network operators must comply with cybersecurity measures, safeguard network operations, and ensure data security (Article 21). These responsibilities include reporting significant cybersecurity incidents to relevant authorities (Article 25) and providing technical support and assistance to public security for national security and criminal investigations (Article 28).

Personal Data Protection

Emphasis on the protection of personal data requires network operators to adhere to the following principles: lawful, just, and necessary collection and use of personal information (Article 41), explicitly informing individuals about the purpose, methods, and scope of data collection (Article 41), ensuring the confidentiality of personal information (Article 42), and obtaining individuals' consent before collecting and using personal information, except in cases specified by law (Article 41).

Critical Information Infrastructure (CII) Protection

CII operators are subject to additional stringent requirements to ensure the security of critical infrastructure and protect sensitive data: conducting regular cybersecurity risk assessments and reporting the results to relevant authorities (Article 34), storing personal information and important data collected and generated within China on servers located within the country (Article 37), and undergoing security reviews when procuring network products and services that may affect national security (Article 35).

Data Localization and Cross-Border Data Transfer

Strict data localization requirements mandate that personal information and important data collected and generated by CII operators within China must be stored domestically (Article 37). Cross-border data transfers are subject to security assessments and must comply with regulations set by relevant authorities (Article 37).

Implications for global data access and compliance

The CSL exerts a significant influence not only within China but also on global cybersecurity practices. Multinational companies are prompted to adopt rigorous cybersecurity measures and data protection protocols to comply with the CSL's stringent requirements. This adaptation often involves substantial adjustments in their data handling and storage practices, as well as enhancements in their overall cybersecurity frameworks to ensure compliance with Chinese regulations.

Violations of the CSL can result in substantial penalties, including fines, suspension of business activities, and revocation of business licenses (Article 66). Specific penalties include fines ranging from RMB 50,000 to RMB 500,000 for network operators that fail to fulfill cybersecurity obligations (Article 59) and fines up to RMB 1,000,000 for serious violations involving the illegal collection, use, or disclosure of personal information (Article 64).

As the global digital environment continues to evolve, the CSL is poised to play an increasingly critical role in shaping the future of cybersecurity and data governance. Its impact is expected to extend beyond China's borders, influencing international standards and practices. The CSL's emphasis on data localization, stringent security reviews, and robust personal data protection sets a precedent that could inspire similar regulatory approaches in other jurisdictions. As China continues to establish itself as a major AI hub, the CSL will be instrumental in shaping the regulatory landscape for AI development and deployment, ensuring that data security and governance are integral components of China's growing influence in the AI sector.

Section II – Deep Dive

South Africa's Protection of Personal Information Act (POPIA)

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

South Africa's Protection of Personal Information Act (POPIA), enacted in 2013 and effective from 2021, governs the processing of personal data within South Africa. The law outlines various requirements and obligations for responsible parties including data controllers and operators involved in handling personal data and maintaining data security. To complement these measures, the South African government published the National Cloud and Data Policy in April 2021 as a further step towards data sovereignty.

Core provisions: data protection

Accountability

Those responsible for lawful processing of personal data must comply with the conditions stated in POPIA for determining the purpose of processing and during processing (Section 8).

Process limitation

Parties must clearly define their purpose for collecting personal data, destroy data after use, and obtain consent from the data subject before processing (Sections 9-12).

Purpose specification

If data is to be used outside the initial purpose, parties must specify the new purpose and duration (Sections 13-14).

Openness

Data collectors must record all processing activities, specify reasons for data collection, identify involved parties, state access rights for data correction/deletion, and indicate if data will be transferred to third parties (Sections 17-18).

Security safeguards

Personal information must be secured to maintain integrity, confidentiality, and prevent data breaches (Sections 19-22).

Data subject participation

Data subjects must be informed of their rights and allowed to alter their data as they see fit (Sections 23-25).

Implications for global data access and compliance

POPIA restricts the transfer of personal information to third parties located outside South Africa unless the receiving party provides an adequate level of protection for the personal information, similar to POPIA (Section 72). Transfers are permitted if the data subject consents, the transfer is necessary for the performance of a contract, or the transfer benefits the data subject (Section 72). Additionally, POPIA regulations state that data cannot be transferred to a foreign country unless it aligns with the EU General Data Protection Regulation, there are binding corporate rules ensuring data protection, a clear written agreement exists between the sender and receiver, and the data subject consents to the transfer.

Violations of POPIA can result in financial or legal penalties, including fines and imprisonment. Specific penalties include fines of up to ZAR 10 million for responsible parties that fail to comply with POPIA's obligations or up to 10 years for offenses involving the unlawful processing of personal information (Section 107).

By emphasizing data safeguards, POPIA strengthens South Africa's economic competitiveness, attracting international businesses and investors that prioritize strong data governance. With secure cross-border data flows and a focus on digital transformation, South Africa can position itself as a regional hub for data processing and management. This approach fosters trust in digital services, while also driving technological innovation and promoting economic growth both within the country and across the region.

Section II – Deep Dive

Saudi Arabia's Personal Data Protection Law (PDPL)

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The Personal Data Protection Law (PDPL) of Saudi Arabia, enacted in 2021, is designed to govern the processing of personal data within the Kingdom. PDPL aims to protect the privacy of individuals and regulate the collection, processing, and storage of personal data by public and private entities. The law outlines various requirements and obligations for data controllers and processors involved in handling personal data and maintaining data security.

Core provisions: data protection

Data collection and use

Personal data must be collected for specific, clear, and lawful purposes, and must not be used in ways incompatible with those purposes.

Consent

Explicit consent from data subjects is required for the collection, processing, and sharing of their personal data, except in cases specified by law.

Data subject rights

Individuals have the right to access, correct, and delete their personal data, as well as object to its processing and request data portability.

Data security

Data controllers and processors must implement appropriate technical and organizational measures to ensure data security and prevent breaches.

Data breach notification

Entities must notify the regulatory authority and affected data subjects of any personal data breaches that could impact data subjects' rights.

Data transfer restrictions

Transfers of personal data outside Saudi Arabia are restricted and require the approval of the regulatory authority, ensuring adequate protection levels.

Implications for global data access and compliance

PDPL mandates that personal data collected within Saudi Arabia must be stored within the country, unless explicit permission is granted by the regulatory authority for cross-border transfers. These transfers are allowed only if the receiving country provides an adequate level of data protection or if sufficient safeguards are in place.

PDPL requires organizations with Saudi Arabia to adopt rigorous data protection measures to comply with its requirements. This involves substantial adjustments in data handling and storage practices and enhancements in overall data protection frameworks. Violations of PDPL can result in substantial penalties, including fines of up to 3 million SAR for entities that fail to comply with PDPL's obligations and potential imprisonment for serious violations involving the unlawful processing of personal data (Article 35).

Section II – Deep Dive

Brazil's General Data Protection Law (LGPD)

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The General Data Protection Law (Lei Geral de Proteção de Dados, LGPD), adopted in Brazil in 2018 and effective from 2020, governs the processing of personal data within Brazil. The law aims to promote the protection of personal information processed by both public and private entities, balancing the right to privacy with other rights and interests.

Core provisions: cybersecurity and data protection

Lawful basis for data processing

Outlines legal bases for processing personal data, including consent, legal obligations, public policies, research, contracts, and credit protection (Articles 7 and 11).

Data subject rights

Grants rights to access, correct, delete data, data portability, and be informed about data sharing (Articles 17-22).

Data protection officer

Requires appointment of a DPO to oversee compliance and act as a contact point for data subjects and the national data protection authority (ANPD) (Article 41).

Data localization and cross-border data transfer

Restricts data transfer to countries without adequate data protection, with exceptions for consent, contract performance, or public interest (Articles 33-34).

Implications for global data access and compliance

Brazil primarily modeled the LGPD after the GDPR to align with international data protection standards and facilitate business operations with global partners. The LGPD shares many principles with the GDPR, such as data subject rights, the requirement for a Data Protection Officer, and stringent conditions for data processing and cross-border transfers. However, there are key differences and regional specificities. The LGPD considers Brazil's unique legal and cultural context, ensuring that data protection measures are compatible with local practices and legal norms. Unlike the GDPR, which is overseen by multiple Data Protection Authorities across EU member states, the LGPD establishes a single national authority (ANPD) to oversee and enforce compliance. Additionally, the LGPD provided a longer adaptation period for organizations to comply compared to the GDPR, reflecting the varying levels of data protection maturity among Brazilian organizations.

The LGPD requires organizations to adopt rigorous data protection measures to comply with its requirements. This adaptation often involves substantial adjustments in data handling and storage practices, as well as enhancements in overall data protection frameworks to ensure compliance with Brazilian regulations. Violations of the LGPD can result in substantial penalties, including fines and other administrative sanctions. Specific penalties include fines of up to 2% of an organization's revenue in Brazil, limited to a maximum of R\$50 million per infraction, as well as other sanctions such as blocking the personal data related to the infraction until it is rectified (Article 52). The LGPD represents a significant step forward in data protection for Brazil, promoting both domestic and international confidence in the country's data governance standards.

Section II – Deep Dive

Further analysis

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The GDPR, CSL, CLOUD Act, LGPD, PDPL, and POPIA each impose unique and significant regulations that impact AI development and data sovereignty, particularly concerning data localization, operational compliance, and the international flow of data through data centers.

The GDPR, with its stringent data protection rules, requires that personal data of EU citizens be processed with high standards of privacy, influencing AI systems to incorporate data minimization and transparency principles. This often requires establishing data centers within the EU to comply with localization mandates. Meanwhile, the CSL mandates that personal information and critical data generated in China be stored locally, significantly impacting AI operations by restricting cross-border data flows and requiring localized data storage and processing capabilities within China. In contrast, the CLOUD Act allows U.S. law enforcement to access data stored overseas by U.S.-based companies, creating a complex compliance environment. AI operations must ensure they can meet U.S. data access requests while also adhering to the data protection laws of other jurisdictions.

Brazil's LGPD imposes similar requirements to the GDPR, emphasizing the protection of personal data and requiring companies to adopt stringent data privacy measures, including data localization under certain conditions. Saudi Arabia's PDPL mandates that personal data be processed with the highest level of security and privacy, affecting how data is stored and managed within its borders. South Africa's POPIA also emphasizes the protection of personal information, impacting AI operations by requiring compliance with local data protection standards and potentially necessitating data localization.

Collectively, these regulations underscore the importance of data sovereignty, requiring AI developers and operators to strategically manage data localization, ensure compliance with multiple regulatory frameworks, and navigate the international flow of data through geographically diverse data centers, balancing legal obligations with operational efficiency and data security.

Analyzing these regulations through the lenses of privacy, protectionism, efficiency, and hybrid approaches clarifies how various data governance models and sovereignty strategies shape AI ecosystems. These perspectives highlight the underlying priorities and trade-offs each region navigates in regulating AI development and data management.

Privacy

Different data sovereignty frameworks are largely shaped by the economic conditions and overall policy outlook of their respective regions. In areas with robust digital economies, such as the EU, data protection frameworks like the GDPR emphasize privacy and human rights. Regions that model their regulations after the GDPR, such as Brazil with its LGPD, and South Africa with its POPIA, prioritize stringent data protection measures to safeguard individual privacy, impacting how data can be transferred and processed through data centers. This regulatory focus balances the need for security and privacy with the potential for innovation and economic growth, reinforcing AI sovereignty by ensuring that AI development adheres to local laws and priorities.

Protectionism

In contrast, some countries adopt data sovereignty frameworks that emphasize national security and protectionism. China and India, with rapidly growing digital sectors, often implement data localization requirements to ensure that critical data remains within national borders. For instance, China's CSL mandates that personal and critical data collected within China be stored domestically, directly impacting the development and operation of local data centers. Saudi Arabia's PDPL also reflects a protectionist stance, requiring stringent controls over how personal data is processed and stored within the country. This approach aims to bolster national security and support local industries by compelling international companies to invest in local data infrastructure.

Although these measures promote local technological advancements, these can also pose challenges for operational efficiency and global business operations, particularly for AI systems that rely on diverse datasets for training and deployment. By controlling the flow of data and requiring local storage, these countries assert AI sovereignty, ensuring that AI technologies develop under the nation's regulatory and security frameworks.

Efficiency

Countries with a significant focus on fostering economic efficiency and innovation, such as the United States and Canada, tend to develop data sovereignty policies that facilitate the free flow of data across borders. These frameworks prioritize the operational efficiency of multinational companies and the seamless integration of global markets. Notably, the CLOUD Act enables law enforcement to access data stored abroad through bilateral agreements, streamlining the process of data access while incorporating privacy safeguards. This approach allows for the efficient operation of data centers globally, supporting AI systems that require quick access to vast amounts of data. By promoting the free flow of data, these countries support the development and deployment of AI technologies across borders, balancing data accessibility with regulatory compliance, thus influencing AI sovereignty by allowing AI systems to leverage global data resources while adhering to international agreements.

Hybrid

In some regions, hybrid and balanced approaches are adopted to reconcile the various demands of data protection, security, and economic growth. Japan and South Korea, for instance, have developed frameworks that permit data transfers under specific conditions while ensuring high standards of data protection. These balanced policies aim to support international business operations and innovation without compromising the security and privacy of personal data. Data centers in these regions must comply with stringent local regulations while facilitating international data flows, supporting AI systems that benefit from both local and global data sources. These hybrid approaches contribute to AI sovereignty by enabling countries to maintain control over AI development within their regulatory frameworks while participating in the global AI economy.

Ultimately, while specific strategies and regulations differ, all data sovereignty frameworks grapple with the core themes of data availability, operational efficiency, security, privacy, and innovation and growth. Each framework seeks to create an environment where data can be managed effectively to support a country's or region's economic and security goals, while protecting individual privacy and fostering technological advancement. This management is crucial for the operation of data centers and the development of AI systems, directly influencing how AI sovereignty is asserted and maintained across different regions.

Section III

Economic impacts

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

The surge in global demand for data is driving significant shifts in how nations approach data sovereignty, influencing economic strategies related to AI infrastructure. Regulatory frameworks governing data, as discussed earlier, play a crucial role in shaping these strategies by setting rules for data handling, cross-border flows, and storage requirements. These regulations not only protect privacy and security but also influence investment decisions in AI development and infrastructure, affecting economic growth and technological innovation worldwide. This section offers an overview of the AI ecosystem and explores the economic implications of data and AI sovereignty.

The POLITICO Research and Analysis Division interviewed 5 leading experts across sectors to provide a comprehensive understanding of these impacts and future trends in the field. The experts include Dr. Vili Lehdonvirta, Professor of Economic Sociology and Digital Social Research at the Oxford Internet Institute; Dr. Tobias Feakin, Australia's former Ambassador for Cyber Affairs and Critical Technology and Founder of Protostar Strategy; Afshin Molavi, Senior Fellow at the Foreign Policy Institute of the Johns Hopkins University School of Advanced International Studies (SAIS); Amir Ghavi, technology and intellectual property law expert and Partner at Fried Frank; and Alex Trafton, interviewed before his current role as SVP for Technology Risk Management at G42 (started August 2024) and formerly Senior Managing Director at Ankura.

Collectively, these experts highlight a growing trend toward data localization, driven by concerns over data security, privacy, and national sovereignty, which in turn creates both opportunities and challenges for businesses and governments. Many emphasize the need for harmonizing global standards to reduce compliance costs and promote innovation, while balancing local regulatory requirements and geopolitical considerations. Striking this balance is essential for creating a predictable and supportive environment for investment and technological progress. The experts agree that the interplay between global coordination and local sovereignty will significantly shape the future of AI development and its economic impact, influencing which regions emerge as leaders in this rapidly evolving field.

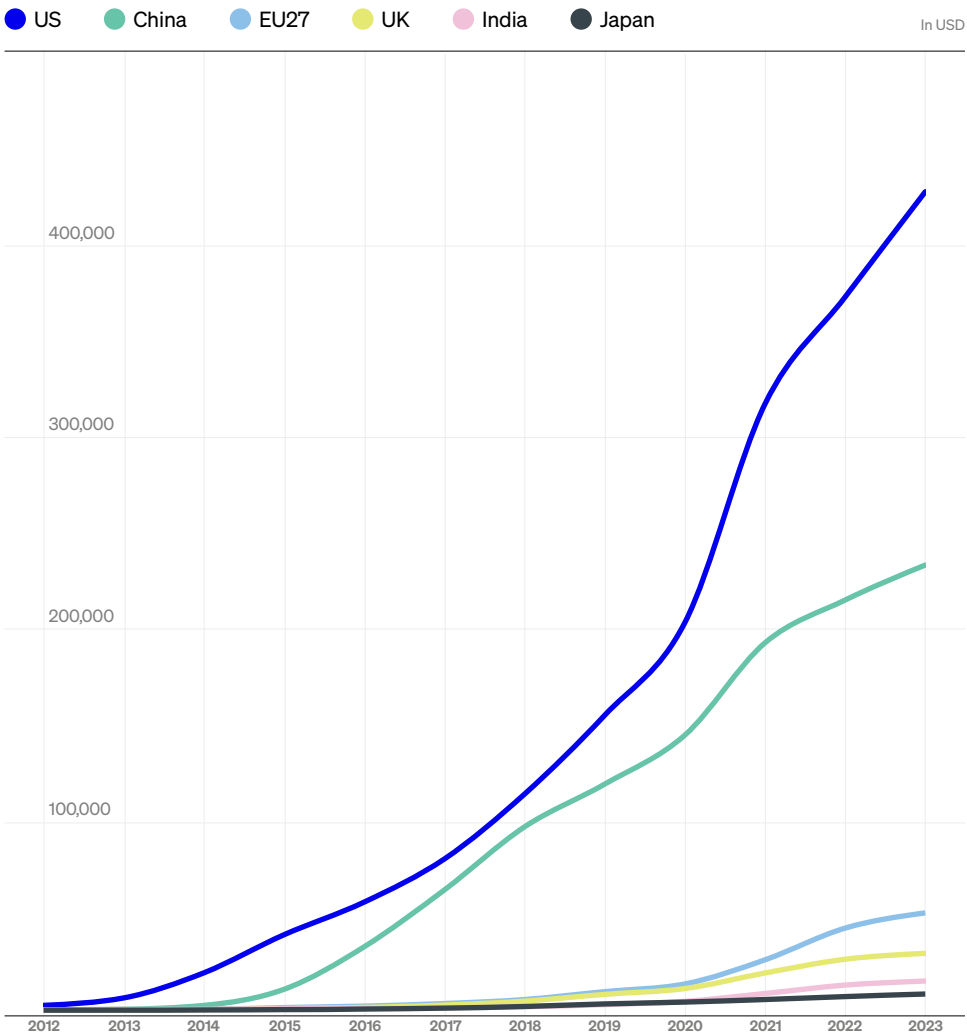
Investment patterns in AI development

Investment trends in AI development are shaped by a combination of regulatory environments, economic stability, and regional innovation capacity. Different countries and regions have adopted varied approaches to AI regulation and digital governance, which in turn impacts where and how companies decide to allocate resources for AI development and infrastructure.

The distribution of AI investment worldwide varies significantly, reflecting the regulatory landscapes, economic priorities, and innovation ecosystems of each region. Countries that provide supportive policies, maintain economic stability, and possess robust digital infrastructures tend to attract more substantial AI investments. These favorable conditions not only foster growth in AI capabilities but also help position countries as leaders in the global AI arena.

Betting on intelligence

Cumulative sum of investments in AI startups in USD (\$)



Source

POLITICO analysis based on OECD.AI (2024) data

The United States and China continue to dominate as the primary players in AI investment, due to their established tech sectors, significant capital availability, and supportive government policies. This is reflected not only in financial investment but also in infrastructure, such as the high concentration of supercomputers and data centers in these regions. Both countries have prioritized AI as a strategic sector, resulting in massive investments from both private and public sectors to enhance their capabilities and maintain their leadership positions.

In the EU, AI investment is also growing, driven in part by regulatory frameworks like the GDPR that have set high standards for data privacy and digital governance. These regulations, while creating compliance challenges, have also established the EU as a trusted region for digital innovation. Dr. Lehdonvirta explains that hyperscaler cloud providers are increasingly offering "sovereignty as a service" to meet European demand for data control, highlighting a strategic response to EU regulations that is shaping AI infrastructure investments in the region. Strong digital policies and the push for a coordinated AI strategy have attracted significant investments, especially in countries like Germany, France, and the Netherlands, which are positioning themselves as leading AI hubs within Europe.

Outside of North America and Europe, new AI investment hubs are emerging in regions such as the Middle East, Southeast Asia, and parts of Africa. These regions are increasingly focusing on building their own AI capabilities, spurred by evolving regulatory landscapes that balance local economic priorities with the need to attract foreign investment. Countries like the United Arab Emirates and Saudi Arabia are notable examples, leveraging their financial resources and supportive policies to create environments conducive to AI development. Molavi emphasized the role of "patient capital" in these regions, stating that countries like "the UAE and Saudi Arabia [...] can invest for the long term without the demands of quarterly earnings reports [...] It's the patient capital that's going to win in this game."

The global AI investment landscape is becoming more diversified, reflecting the varying regulatory, economic, and strategic priorities of different regions. Ghavi pointed out, "Different countries have different interests to protect. Some are looking to protect their rich and deep catalogs of media from AI training, while others are looking ahead to aim to attract AI model developers." The motivations behind sovereign approaches to data governance can differ widely; for example, South Africa's more protectionist framework can be interpreted to prevent data extraction by foreign companies and protect local interests, whereas China's protectionist stance on data governance is often seen as a strategy for monitoring information flows and supporting national security. These diverse approaches to data sovereignty will continue to shape the global AI ecosystem, determining which regions emerge as future leaders in AI innovation and development. As these trends evolve, they will likely influence not only regional competitive advantages but also the broader dynamics of global technological leadership.

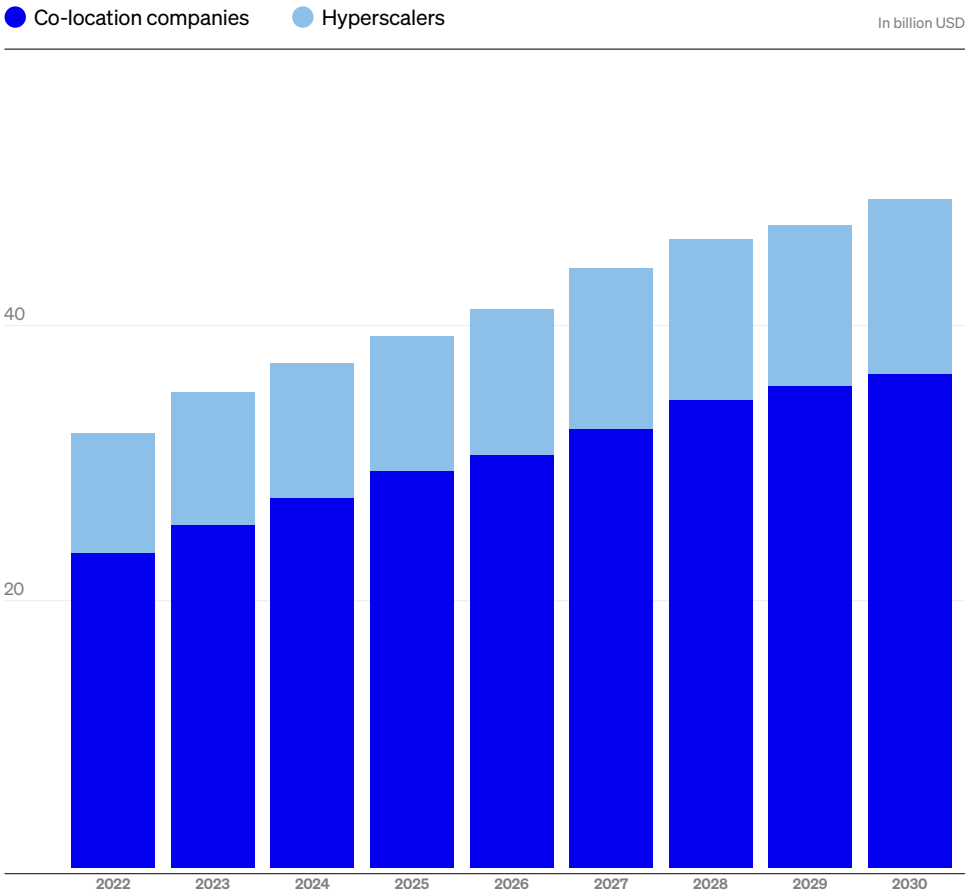
Investment in data center infrastructure

Data needs have been growing exponentially for years, but the infrastructure requirements for AI development and deployment have acted as an accelerant, driving even more rapid expansion in data center investments.

The demand for data centers is closely linked to regulatory requirements for data localization, privacy, and security. As countries implement stricter data governance frameworks, companies are increasingly investing in data center infrastructure that complies with these localized data requirements. Dr. Feakin notes that "due to the avalanche of government data localization policies, there has been a significant impact on the data center industry, especially [...] in terms of the geography of data centers." This trend has resulted in a noticeable shift in where companies are choosing to build and operate their facilities.

Future surge

Projected global spending on data center construction by hyperscalers and co-location companies



Source

McKinsey (2024)

Investment trends indicate that co-location companies, which provide shared data center spaces for multiple clients, currently dominate the market. This reflects the immediate need for local data storage solutions that adhere to specific regulatory mandates tied to data sovereignty. At the same time, there is a balanced increase in investments from both co-location companies and large-scale cloud providers.

This trend demonstrates a maturing market where both local and scalable solutions are being developed to accommodate regional data storage needs and more expansive data processing capabilities. Echoing Dr. Feakin, Dr. Lehdonvirta highlights that "data localization rules do influence location decisions of cloud providers and infrastructure providers when they decide where to locate their major infrastructure." This insight stresses how data sovereignty requirements shape the strategic decisions of tech companies, compelling them to invest in data centers that can both comply with local regulations and support their global operations.

This evolving landscape demonstrates that stringent data protection regulations do not hinder AI development but rather shape the strategies and investments in AI infrastructure. Companies are adapting by building compliant data centers and developing innovative solutions to manage and utilize data within the regulatory frameworks that govern these specific geographies. By aligning AI strategies with local regulations, companies can unlock new opportunities for growth and collaboration, fostering an environment where innovation is driven by both compliance and creativity.

Economic impacts of fragmented data governance

The economic impacts of fragmented data governance and evolving AI infrastructure strategies are creating both challenges and opportunities for companies and regions globally. As companies navigate complex regulatory environments, the cost of compliance becomes a significant consideration. According to Dr. Feakin, "the varied regulatory landscape can increase operational costs by up to 20% due to the need for additional legal compliance checks and potential infrastructure changes." Additionally, Dr. Lehdonvirta emphasizes that these challenges are not only about compliance costs but also about ensuring data flows smoothly across borders to avoid disruption in AI model training and deployment. Dr. Lehdonvirta further adds that while some regions may seek to tighten their data governance policies, others might aim for more permissive regimes, creating a complex patchwork that companies must strategically navigate.

As companies navigate complex regulatory environments, AI infrastructure has emerged as a strategic gateway for expanding into emerging markets. For instance, firms are leveraging data centers and localized AI capabilities to comply with stringent local regulations while also gaining a foothold in new territories. This approach allows them to address unique local challenges—such as GDPR compliance in the European Union or data residency requirements in Asia—by providing tailored solutions that balance regulatory adherence with operational flexibility. By building infrastructure that aligns with specific data sovereignty frameworks, companies are not only ensuring compliance but also positioning themselves strategically to capture growth opportunities in markets with distinct economic and regulatory dynamics.

Ultimately, the interplay between local regulatory demands and global AI governance trends will shape the future landscape of data-driven economic growth. While fragmented data governance increases operational costs and complicates international expansion, the potential for harmonization presents a pathway to lower compliance costs and foster innovation across borders. From his legal perspective, Ghavi notes a convergence around common principles like safety, security, and trust is already being seen through coordinated efforts such as the White House voluntary commitments, the Hiroshima Principles, and the Seoul commitments. These agreements can help create a more predictable regulatory environment that encourages investment and technological development. Additionally, emphasizes Trafton, the "maturation of data security" in this field will also help contribute to an increasingly stable ecosystem. However, the path forward will require a careful balance between accommodating global standards and respecting local sovereignty, allowing companies to navigate the complexities of data governance while driving economic growth and innovation for global powers and emerging markets alike. Successfully managing this balance will be key to fostering a collaborative, innovative, and economically vibrant global AI ecosystem.

Section IV

Sovereign AI ecosystems and the future

This document was researched and produced by the POLITICO Research & Analysis Division independent of the POLITICO newsroom. You receive this document as part of your POLITICO Pro Analysis subscription. For any questions and feedback please contact pro@politico.eu. This document contains privileged, confidential and proprietary information from POLITICO, exclusively intended for internal use. Any unauthorized use, copying, disclosing, forwarding, publishing or redistribution of this document in any way is strictly forbidden. All rights are reserved.

As the global AI ecosystem continues to evolve, the interaction between data governance, AI sovereignty, and technological advancement remains central to shaping its future trajectory. The rise of data sovereignty frameworks, particularly outside of North America and Europe, reflects a broader movement towards asserting national control over data, which has direct implications for AI development, data center operations, and international data flows.

This section synthesizes the report's findings, drawing together data and analysis on the global distribution of data centers and supercomputers, mapping the diverse governance frameworks influencing AI development, and examining the economic factors shaping these trends. It integrates insights from leading experts to provide a holistic understanding of sovereign AI ecosystems, emphasizing the relationship between physical infrastructure, such as data centers, and data governance policies. By exploring how nations and companies manage these elements, this section highlights the strategic approaches required to thrive in a complex and evolving AI landscape. The subsequent sections convey some of the key insights of the report, offering a comprehensive view of how AI sovereignty, regulatory frameworks, and infrastructure investments are interconnected and shaping the future of AI globally.

Legislative frameworks as pillars of AI sovereignty

Legislative frameworks, such as the GDPR, CSL, CLOUD Act, and their counterparts across regions, serve as the foundational structures defining data sovereignty in the context of AI development. These laws dictate the rules for data handling, storage, and cross-border transfers, emphasizing privacy, security, and compliance. As a result, companies must adapt by localizing data storage, implementing robust data governance policies, and ensuring that AI systems are developed in accordance with local regulations. The widespread adoption of these frameworks underscores the need for nuanced strategies that balance regulatory adherence with operational flexibility.

Data centers and the localization imperative

Data centers have emerged as critical components of AI infrastructure, facilitating compliance with data localization laws and supporting the computational needs of AI systems. The global distribution of data centers reflects varying regional approaches to data sovereignty, with countries such as the United States, China, India, and the UAE investing heavily in localized infrastructure. These investments are not merely reactions to regulatory requirements but strategic moves to bolster national security, economic growth, and technological competitiveness. The localization of data centers also promotes regional expertise in managing data flows within secure and compliant frameworks, which is essential for maintaining public trust and fostering innovation.

This investment landscape is also transitioning. As AI capabilities become more advanced, the requirements for data processing and storage are increasing, driving a need for more sophisticated and scalable data centers. The movement from traditional data centers to hyperscaler and edge computing facilities is accelerating, enabling more efficient data processing closer to where it is generated and needed. This evolution is crucial in managing the vast amounts of data required for AI systems while adhering to local regulatory mandates.

Global data flows and the challenge of harmonization

The fragmentation of global data governance presents both challenges and opportunities for the AI sector. Diverging regulations increase operational costs and complicate international expansion, but they also incentivize the development of innovative, region-specific solutions that align with local laws. Harmonizing data governance standards across regions could lower compliance costs, streamline data flows, and foster global innovation. However, achieving such harmonization requires balancing national sovereignty with international cooperation, a complex endeavor given the varied economic, political, and security interests at play.

Future trends in AI sovereignty: strategic investments and technological innovation

Looking ahead, AI sovereignty will increasingly encompass not just data sovereignty but also control over AI algorithms, infrastructure, and hardware. Nations are prioritizing investments in AI infrastructure, such as data centers and supercomputing facilities, to build independent AI capabilities and reduce reliance on foreign technology. Strategic capital deployment, particularly by state-backed entities, underscores the importance of building domestic AI ecosystems that support local innovation and provide opportunities for global expansion.

The transition in the AI landscape is marked by a shift from reactive to proactive strategies in building these ecosystems. Countries are no longer merely responding to external pressures; they are actively shaping their AI futures through long-term planning and investments. This approach extends beyond infrastructure, encompassing human capital development, research and innovation, and the cultivation of ecosystems that support AI startups and innovation. By taking a proactive stance, countries are positioning themselves as leaders in the next phase of AI development.

Encryption and data security

As data security and privacy become core components of AI sovereignty, advanced encryption and cryptographic techniques will be crucial for protecting sensitive data across sectors. Regulatory requirements around data privacy will drive the demand for robust encryption strategies, particularly in industries like healthcare and finance, where the stakes are highest. Companies that develop strong encryption capabilities will not only navigate complex regulatory landscapes more effectively but also protect their intellectual property and maintain competitive advantages in the global market.

Navigating a fragmented future: balancing global coordination and local sovereignty

The future of AI development will be shaped by how nations and companies navigate the complexities of fragmented data governance frameworks while leveraging strategic opportunities in AI infrastructure. Tailored, unique solutions that meet local regulatory demands are essential for companies operating in a range of global contexts. As global standards evolve and local expertise only continues to develop, finding a balance between international coordination and respect for local sovereignty will be key to driving sustainable innovation and economic growth in the AI sector.

The path forward for sovereign AI ecosystems will require thoughtful strategies that integrate legal compliance, technological innovation, and international collaboration. By embracing these dynamics, nations and companies alike can foster resilient and competitive AI ecosystems that support their long-term economic and strategic objectives.

