FEBRUARY 2026

POLICY BRIEF

# INTERNATIONALLY FRAGMENTED DATA COULD LEAD TO GEOPOLITICALLY ANTAGONISTIC AI

HUNG TRAN

POLICY CENTER FOR THE NEW SOUTH

PB - 08/26

POLICY CENTER FOR THE NEW SOUTH

*Divergent regulatory regimes for data, driven by different motivations, ranging from privacy protection in the European Union to information control in China, could eventually produce distinctively different, and possibly contradictory, bodies of data. Artificial-intelligence models trained on those datasets could produce differing and possibly even conflicting outputs. To the extent that AI outputs start to shape human perception and to influence decisions, in governments and businesses, and among the public, antagonistic AI models would reinforce the mutual mistrust and hostility inherent in the current geopolitical environment, potentially making it harder to resolve conflicts. As a consequence, the fragmentation of data is becoming an important issue in the evolution of AI and its potential impact on human society.*

**HUNG TRAN**

# INTRODUCTION

Impressive progress continues to be made in artificial intelligence (AI). The use of AI applications in daily life is increasing, from sophisticated chatbots to self-driving taxis, such as those operated by Alphabet's Waymo in the United States, or Baidu's Apollo Go in China. More importantly, AI is evolving from generative AI to , becoming more autonomous. In this context, public debate about AI's potential benefits and costs—or negative consequences—has understandably intensified. Many thinkers, policymakers and business leaders have called for globally coordinated governance frameworks to promote AI innovation and development within secure guardrails, in order to minimize the risk of bad outcomes.

However, heightened geopolitical contention has led to division and fragmentation instead of internationally coordinated action. Most noticeable has been the fragmentation of international trade and investment flows. Increasingly, in the emerging legal and regulatory frameworks for AI in major jurisdictions. In addition to working in line with their different national values and cultural/social orientations—or home biases—many powers have tried to assert AI sovereignty as part of their strategic efforts to win the AI race. This is seen as vital especially to safeguard national security in the context of geopolitical competition—but is intensifying AI fragmentation in the process.

'AI sovereignty' refers to a country's ability and willingness to develop the whole AI stack using its own infrastructure, including digital infrastructure and manufacturing capacity, data, workforce, and business networks. Among these components, data sovereignty can be established more readily by national laws and regulations, compared to the effort and costs involved in developing AI infrastructure and manufacturing capacity. Moreover, data have become the new oil in the digital/AI age. Understandably, data sovereignty has become a strategic goal for many countries—including those beyond the small circle of major powers—which want to gain some oversight over the use of data, and hopefully AI applications, in their jurisdictions.

The three most important jurisdictions in the world are the U.S., China, and the EU. China strictly controls both the inflow and outflow of information, while the EU is keen on the protection of personal data privacy and fact-checking of misinformation on social media. The U.S., meanwhile, does not have a comprehensive federal personal data protection law, though some U.S. states have implemented their own laws. Importantly, the administration of U.S. President Donald Trump views fact-checking as a form of censorship, effectively allowing all types of information—including misinformation—to circulate online. Other jurisdictions besides those three have also implemented regulations on data collection and transfers.

*Divergent data regulatory regimes, driven by different motivations, ranging from privacy protection in the EU to information control in China, could eventually produce distinctively different, and possibly contradictory, bodies of data. AI models trained on those bodies of data could produce outputs that differ* from, and even conflict with, one another. To the extent that AI outputs shape human perception and influence decisions—in governments, businesses, and among the public—*antagonistic AI models could reinforce the mutual mistrust and hostility* inherent in the current geopolitical contention, potentially making it more harmful and difficult to navigate. As a consequence, fragmented data have become an important issue in the evolution of AI, and its potential impact on human society.

## AI and Data Sovereignty

AI sovereignty has been understood to be the control, if not ownership, of the whole stack of the AI value chain, so that a country can remain autonomous in making decisions on AI and other matters, without being subject to undue pressure from other powers. According to the World Economic Forum, the AI stack has six key components: foundational inputs (i.e. electricity), raw materials (such as silicon), hardware inputs (i.e. semiconductors), infrastructure (including compute, clouds, and data centers), data and foundation models, and applications and services. These components are supported by key enablers: AI strategy, enabling of adoption, fundamental R&D and innovation, talent and skills, access to capital, and enabling technologies (i.e. devices, connectivity, and cybersecurity).

For advanced economies that already have strong foundations in science, technology, and innovation, plus manufacturing capacity and digital infrastructure, securing leadership positions in all of the six AI ecosystem components would require trillions of dollars in investment, especially in data centers that use significant amounts of energy. This is simply out of reach for many countries. Many of those countries thus aim to focus on the downstream parts of the AI value chain, especially the generation, use, and (cross-border) transfer of data; the testing of foundation models; and regulatory requirements for AI applications and services within their jurisdictions. They expect these measures to give them a degree of regulation of, and oversight over, the use of AI by their citizens.

## Implications of Divergent Data Regulatory Regimes

Data and cross-border data flows have become vital parts of the global economy. For example, the data-transfer relationship in trades between the U.S. and Europe is worth $7.1 trillion. However, national policies and the regulatory regimes that govern the generation, storage, processing, and cross-border transfer of data—both personal and national security-related—have diverged, increasingly driven by geopolitical contention. These regulatory divergences imply internationally fragmented bodies of data, with serious implications for the quality of data needed to train AI models. Conceptually, this could lead to geopolitically antagonistic AI systems used by different major powers.

In particular, differences among the three major jurisdictions mentioned above have become significant.

### European Union (EU)

The EU adopted the General Data Protection Regulation (GDPR) in 2016, giving EU residents significant control over their personal data (including the right to request deletion of their data); standardizing data protection across member states; and extending the rules to any entities around the world handling EU personal data. The GDPR includes strict rules on collecting, storing, processing, and transferring personal data, especially cross-border. Data transfers to countries outside the European Economic Area (EEA) can take place freely only to those—including the UK, Japan, Switzerland and several others—deemed as "*offering an adequate level of data protection*" by the European Commission under the EU Data Privacy Framework (DPF). US commercial organizations also participating the DPF. Where such blanket adequacy recognition is not in place, foreign entities engaging in data transfer need to satisfy specific safeguards such as Standard Contractual Laws (SCL) or Binding Corporate Rules (BCR), ensuring adequate data protection by those entities.

More relevant for AI training data is the EU AI Act (2024), which requires developers of general purpose AI to publish detailed reports on the content used to train AI models, so that copyright holders and regulators can monitor their compliance with data protection laws and regulations.

Equally importantly, the EU Digital Services Act (DSA, 2022) enforces strict rules on digital online intermediaries, including social media platforms and search engines, to combat illegal content, disinformation, cyber harassment, advertisements targeting minors, and algorithmic profiling.

Generally speaking, strict data-protection regulations with extraterritorial reach, as implemented by the EU, tend to impose costs and raise hurdles in AI development, and could come into conflict with regulatory approaches of other major jurisdictions, in particular the U.S.

## China

China has passed several laws governing data localization and cross-border transfer, data audit, and data security, with a clear focus on protecting national security and with an extraterritorial reach.

Specifically, the Personal Information Protection Law (PIPL, 2021) is somewhat similar to the GDPR in highlighting the rights of persons over their personal data, including the right to give consent for corporate use, and regulation of the storage and processing of personal data by entities inside and outside of China, with strict rules for cross-border data transfer. The Data Security Law (DSL, 2021) mandates strict controls, localization, and approval for cross-border transfers of data deemed relevant for national security and economic interests. The Cybersecurity Law (CSL, enacted in 2017 and amended in 2025) focuses on national security, data sovereignty, and data localization for critical information infrastructure operators. In 2025, the Network Data Security Management Regulation was passed to update and expand the above mentioned laws, putting them into a comprehensive framework.

It is important to recognize that these laws are there to formalize the effective control of the Communist Party of China over the generation and dissemination of data and information in China. In particular, access to the internet has been tightly controlled, with many foreign websites banned, while approved domestic websites are promoted—. Moreover, generative AI must not contain content that violates China's core socialist values, as measured by the country's cybersecurity standards committee. Generally speaking, incoming information has always been subject to firewalls and censorship, while there is a requirement for outgoing information to conform with regulations and to be vetted by Chinese authorities. As a result, there is a growing difference between the domestic content available to Chinese citizens, and the international information about China allowed for consumption by the rest of the world.

Last but not least, according to the National Intelligence Law (2017), China's security authorities have the power to access all data and information, no matter where stored, on Chinese organizations and individuals, operating domestically as well as internationally.

## The United States

By contrast, the U.S. has adopted a relatively *laissez-faire* approach to privacy protection, with no comprehensive federal regulations on protecting personal data privacy, except for a few specific cases. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects patient health information from disclosure without consent, covering entities such as healthcare providers, insurers, and clearing houses (which process, reformat and transmit sensitive patient data). The Children's Online Privacy Protection Act of 1998 (COPPA) protects the online privacy of children under 13, requiring operators of websites or online services targeting children to obtain parental consent before collecting personal information. The most recent rule is the Department of Justice 2025 Final Rules based on Executive Order 14117 restricting the bulk transfer of sensitive personal data and government related data to countries of concern (including, for example, China, Russia, and Iran) for national security reasons.

In addition to those federal regulations, around 20 U.S. states (including California, Virginia, Florida, and Texas) have passed comprehensive data-privacy laws—mostly in 2024 and 2025. These state laws form a patchwork of rules, differing in many aspects, including compliance thresholds (in terms of numbers of employees of companies or their revenues), the subjects covered (only customer data, or including employee data and businesses-to-business information, as in California), and enforcement mechanisms. The fragmented regulatory landscape is burdensome for companies doing business in different U.S. states.

Importantly, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed in 2018, allows U.S. law enforcement authorities to compel U.S.-based technology companies, via warrants or subpoenas, to disclose data stored inside or outside the U.S. This law could conflict with data-localization requirements in many countries.

It is important to note that the Trump administration has abandoned many monitoring mechanisms to fact-check information being disseminated publicly, especially via social media platforms, on the basis that it regards such actions as censorship. This could pose a challenge to efforts to clean up and improve the quality of data in the U.S. Importantly, the U.S. views EU digital laws, in particular the Digital Services Act, as imposing 'extraterritorial censorship' and attacking U.S. high-tech companies. The U.S. has imposed sanctions on EU officials involved in promoting and implementing the DSA, and has threatened tariffs. At present, this issue is one of the major points of contention between the U.S. and EU.

# The Search for Data Sovereignty by Other Countries

In addition to the three main AI players—the U.S., China, and the EU—a number of other countries have stated their intentions to achieve data sovereignty for strategic reasons. Among the 36 countries selected by the Stanford Institute of Human-centered Artificial Intelligence (HAI) for their progress in AI development and vibrancy, it is interesting to highlight the examples of India, Brazil, South Korea, and Malaysia, to portray the range of countries and their approaches to AI/data sovereignty, all of which contributes to data fragmentation.

## India

Having grown robustly in recent years, India aims to be one of the world's key economies for AI, with full sovereignty. India ranks third in the HAI list. It has leveraged its strength in the IT services sector, in which the major corporate players have supported R&D efforts, and have built data centers to promote the use of indigenous data. In particular, India has implemented policies to secure its sovereignty throughout the AI supply chain, including R&D, design, software and hardware development, and especially data. This was reinforced by the 2023 Digital Personal Data Protection Act, which requires localization of data and tightens control over use of personal data, including in cross-border exchange. India has also prioritized the protection of intellectual property related to software in recent trade negotiations.

Within the regulatory guardrails, and leveraging its developed digital infrastructure, India has been active in promoting open, interoperable, and comprehensive domestic datasets, which are valuable for specific applications. For example, the Reserve Bank of India has sponsored an Account Aggregator Framework to enable secure, consent-based sharing of financial data across 2.2 billion bank accounts—creating very useful data sets for individual financial transactions. The Ayushman Bharat Digital Mission maintains a unified health data backbone, issuing 830 million digital health IDs, and linking 780 million medical records—useful for predictive and diagnostic applications. In 2025, MeiY launched AIKosha, a national depository of curated datasets and foundation models, for use by startups and researchers.

The datasets thus generated have been used to develop applications. India's Unified Payment Interface (UPI) accommodates up to 20 billion banking transactions a month; these data have been used for AI-powered credit scoring and fraud detection. In healthcare, eSanjeevani has supported 350 million tele-consultations, supporting the development of AI-enabled diagnostics. In agriculture, Agri-Atack and Agriculture Data Exchange help promote AI and remote sensing in crop management and yield forecasting.

In short, India is an example of a balanced approach in protecting data privacy and regulating cross-border transfers, while developing interoperable and comprehensive domestic datasets, supporting AI-powered applications in various areas.

## South Korea

Ranked fourth in the HAI list, South Korea has established a National Artificial Intelligence Strategy Committee, made up of policymakers and private AI business leaders, to formulate and coordinate plans to make the country one of the top three AI powers in the world—a goal that has been articulated by President Lee Jae Myung. The Committee will oversee the whole AI stack: infrastructure, data, applications, social adaptation, global cooperation, science and skill development, and defense and security. The government has pledged 100 trillion won ($68.5 billion) to implement those plans.

South Korea has also passed the Personal Information Protection Act of 2020, one of the strictest such laws in the world, mandating control of citizen data and cross-border transfers. It is complemented by the Network Act (with strict penalties for disseminating false or manipulated information), and the Credit Information Act (with rules for the use and protection of personal credit data in the financial sector). The goal is to develop a strong national digital ecosystem, with digital 'home biases'.

## Brazil

Ranked sixteenth in the HAI list, Brazil is a big and important developing country striving to establish AI and data sovereignty, to ensure national control over AI development in alignment with its national legal and cultural standards. The country is in the process of passing an AI Bill to provide a regulatory framework for AI development, focusing on human-centric, ethical, and transparent AI, accompanied by accountability for providers of AI services. The Bill classifies AI risks into categories that require different levels of regulatory oversight. In particular, it prohibits "excessively risky" AI systems. A National Data Protection Agency will be established to oversee AI governance and compliance.

In the meantime, Brazil is implementing a Strategic AI Plan (PBIA, 2024-2028), budgeting 23 billion Brazilian reals ($4.4 billion) to boost national competitiveness in infrastructure, talent, and research, and for development of advanced language models in Brazilian Portuguese to reflect national, cultural, and social characteristics. In particular, Brazil plans to build domestic data centers, capitalizing on its renewable energy capabilities, with renewables accounting for 87% of the country's electricity generation.

## Malaysia

Malaysia, ranked twenty-sixth in the HAI list—one of the two Southeast Asian nations included in the list, alongside Singapore, which ranks second—offers an interesting example of a small country aspiring to AI sovereignty. Malaysia has adopted a national AI sovereignty strategy, focusing on developing a self-reliant AI ecosystem based on local data (aligned with national culture and values), infrastructure (including Nvidia-powered data centers, compute capacity, and hardware), and talent, through initiatives such as National AI Offices (NAIO), local large language models (LLMs), and investment in local manufacturing. Malaysia aims to become one of the leading AI countries by 2030.

# Implications of Fragmented Data on AI Models and Outcomes

It is unclear if passing national regulations on data usage and privacy protection will be sufficient to enable countries to fully exercise data or AI sovereignty. Many countries, besides the major powers, rely on AI infrastructures such as cloud-based storage, compute and processing services, and foundation models and their applications, which are provided by major high-tech/AI corporations mostly based in the U.S. and China. Moreover, as those two superpowers compete to establish AI standards including norms, technological standards and data governance, countries will be put in a position to choose one of the two alternative standards. These give those governments the ability to leverage access to AI infrastructures, products, and services to influence the decisions of other nations.

However, it seems clear that fragmentation of data, reflecting different national perspectives or home biases, has added an additional layer of difficulty, plaguing raw data that have been used for training AI models. A supposedly global data pool, that, for example, uses all information on the world wide web, would contain many inconsistent and contradictory data points, making it difficult for AI models to formulate coherent and sensible outcomes. On the other hand, nationally approved datasets, resulting from data sovereignty regulations such as localization, restrictive cross-border transfers, and 'spinternet' tendencies related to controls over access to the internet, would become ideological data silos. These could

lead to AI outcomes that reflect national ideological, cultural, and political worldviews, perpetuating biases about other nations and peoples.

The geopolitically driven differences in national datasets complicate the usual problems already plaguing raw data. These include the training of AI models on varied, inconsistent, and contradictory data, potentially reinforcing societal biases inherent in the data, and leading to unfair decisions and outcomes in critical areas such as healthcare, finance, and employment. More serious defects in training AI on problematic data include performance degradation and hallucinations—especially when AI-generated data pollute future training datasets, leading to plausible but factually incorrect outcomes—and model collapse because of loss of fidelity to originally high-quality data after successive rounds of training.

Along with privacy and security risks, possible suboptimal AI outcomes caused by data-quality problems pose the risk of spreading misinformation, potentially intensifying mistrust and political polarization in many countries. This has become a serious concern, as recent and more sophisticated generative AI models have been used to turn out — misinformation and manipulated content through messages, texts, pictures, audio, and video files, increasingly difficult to distinguish from the real equivalents. This can be used to influence consumers in commercial advertisements, and more importantly, to sway voters in political processes and election campaigns.

From a commercial perspective, inaccurate and incomplete information been estimated to cost U.S. businesses about $3 trillion a year. This has made data a competitive challenge for major high-tech companies, driving their efforts to develop highly curated and proprietary datasets to train their AI models—again contributing to data fragmentation.

Normally, these problems could be addressed by data-centric approaches involving cleaning, annotating, and improving data quality throughout the lifecycle to improve the training of AI models. Techniques including data augmentation (like rotation and adding noise to combat limited data), regularization (using regression techniques to overcome overfitting in sparse data), and robust curation, auditing, and monitoring to address biases and misinformation, can also be used. Generally speaking, while the latest AI models, such as Open AI GPT-5, Google DeepMind Gemini-3, Anthropic Claude 3.7, xAI Grok 3, DeepSeek-R1, and Qwen QWQ-32B, have made progress in handling messy and unstructured data, 'garbage in, garbage out' remains a feature of AI, as with any digital process.

## Impacts of Fragmented Data

Importantly, no curation can deal with the policy-driven differences intentionally embedded in national datasets. Consequently, AI models trained on global datasets that contain contradictory national data points will suffer from the problems of raw data described above. The AI models trained only on nationally-approved data would reinforce the biases and antagonistic perceptions of the originating country relative to other competing nations.

To the extent that AI outcomes increasingly influence human perceptions and decision making, and become increasingly embedded in daily life, these trends are worrisome. They perpetuate and reinforce mutual mistrust, undermining the willingness to cooperate internationally. More importantly, as AI has increasingly reshaped the conduct of warfare, especially in mission command—having timely access to critical data and analysis—any biases in AI outputs could have serious consequences. For example, without rigorous and

effective control by humans, those outputs could lead to decisions and actions that could inadvertently trigger unwanted and unexpected military escalation and armed conflict.

Developing countries that are unable to fully exercise AI/data sovereignty must rely on AI products and services provided by foreign companies. They are forced to use AI models and outputs not adequately based on their national data, but reflecting the biases in data used to train those models. Such AI outcomes may not be consistent with their own values and perspectives. Furthermore, the heightened U.S.-China technological and AI competition, as part of the overall geopolitical conflict dubbed "the New Great Game", could deepen the digital fragmentation and widen the global AI divide between themselves and many developing countries. Worse, many countries may be forced to choose either U.S.-centric or China-centric AI ecosystems including competing standards. This could skew public sentiment in developing countries more closely to one of the two geopolitical competitors, making it difficult to mobilize public support for a policy of non-alignment, though it may be in their long-term national interests.

In short, fragmentation of data along national values and perspectives, or home biases, could lead to geopolitically antagonistic datasets. AI models trained on those data could then produce results that influence human perception and decisions, possibly in ways that intensify mutual mistrust inherent in current geopolitical contention, and making it more harmful and harder to navigate.

# ABOUT THE AUTHOR

## HUNG TRAN

Hung Tran is a senior fellow at the Policy Center for the New South, a nonresident senior fellow at the Atlantic Council's GeoEconomics Center; and a former executive managing director at the International Institute of Finance and former deputy director at the International Monetary Fund.

# ABOUT THE POLICY CENTER FOR THE NEW SOUTH

The Policy Center for the New South (PCNS) is a Moroccan think tank aiming to contribute to the improvement of economic and social public policies that challenge Morocco and the rest of Africa as integral parts of the global South.

The PCNS pleads for an open, accountable and enterprising "new South" that defines its own narratives and mental maps around the Mediterranean and South Atlantic basins, as part of a forward-looking relationship with the rest of the world. Through its analytical endeavours, the think tank aims to support the development of public policies in Africa and to give the floor to experts from the South. This stance is focused on dialogue and partnership, and aims to cultivate African expertise and excellence needed for the accurate analysis of African and global challenges and the suggestion of appropriate solutions. Read more



**Policy Center for the New South**

Rabat Campus of Mohammed VI Polytechnic University,
Rocade Rabat Salé - 11103
Email : contact@policycenter.ma
Phone : +212 (0) 537 54 04 04
Fax : +212 (0) 537 71 31 54

**www.policycenter.ma**

POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE