BIPSS Commentary
www.bipss.org.bd
July-2024
BIPSS
Towards a Secure World

Digital Sovereignty: Balancing Innovation and Security in the Age of AI

Sirat-E-Rowshan Islam[1]

Introduction

The rapid advancement of artificial intelligence (AI) technologies has introduced us to a new era of both tremendous opportunity and significant risk. AI-powered systems have the potential to drive innovation, boost economic productivity, and tackle complex global challenges. At the same time, the proliferation of these technologies has raised pressing concerns around data governance, cybersecurity, and the ethical deployment of AI.

Source: Dev Community

So, what is digital sovereignty? In the digital economy, cloud services are becoming increasingly important to be able to use, transfer and store data in a way that is safe and secure. In this emerging

[1] Sirat-E-Rowshan Islam is a Research intern at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS in from the Bangladesh University of Professionals (BUP).

landscape, digital sovereignty is about how a state regulates and exercises control over the technology and services in use there. It’s concerned with keeping sensitive data secure and enabling businesses, organizations, and individuals to enjoy greater autonomy over their digital assets and data. Simply put, it’s about controlling where the data resides, where it flows, and who has control over it.[2] In this context, the concept of "digital sovereignty" has gained increasing prominence on the security concerns of countries around the world

Emergence and Relevance of Digital Sovereignty

Over the past decade, we have used digital as a welcome innovation to change how we relate to others, conduct business and connect to institutions. The pervasiveness of the Internet, the emergence of social media, the different ways we receive information, and so many other habits have been changed through this innovation.[3]

In the early stages of the internet, the digital space was largely unregulated, with a strong emphasis on openness and global connectivity. The United States played a significant role in the development of internet infrastructure and governance through institutions like the Internet Corporation for Assigned Names and Numbers (ICANN). The modern data economy is growing at a rapid pace. The EU Commission estimates that the volume of data produced in the world will increase from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025. Every 18 months, the amount of data is doubling. At the same time, according to EU’s estimates, the value of the data economy will increase to over €550 billion by 2025, representing 4% of the overall EU GDP. [4]

In recent years, geopolitical tensions have intensified the focus on digital sovereignty. Concerns over espionage, cyberattacks, and foreign influence in domestic affairs have led countries to reevaluate their dependence on foreign technology providers. The United States' restrictions on

[2] Wenche Karlstad, “Digital Sovereignty - What, Why and How?,” n.d. https://www.tietoevry.com/en/blog/2023/05/all-you-need-to-know-about-digital-sovereignty/.

[3] Antonio Grasso, “Digital Sovereignty: What It Means and Why Governments Consider Data and Digital Technologies Strategic Infrastructure,” December 5, 2022, https://www.linkedin.com/pulse/digital-sovereignty-what-means-why-governments-consider-grasso/.

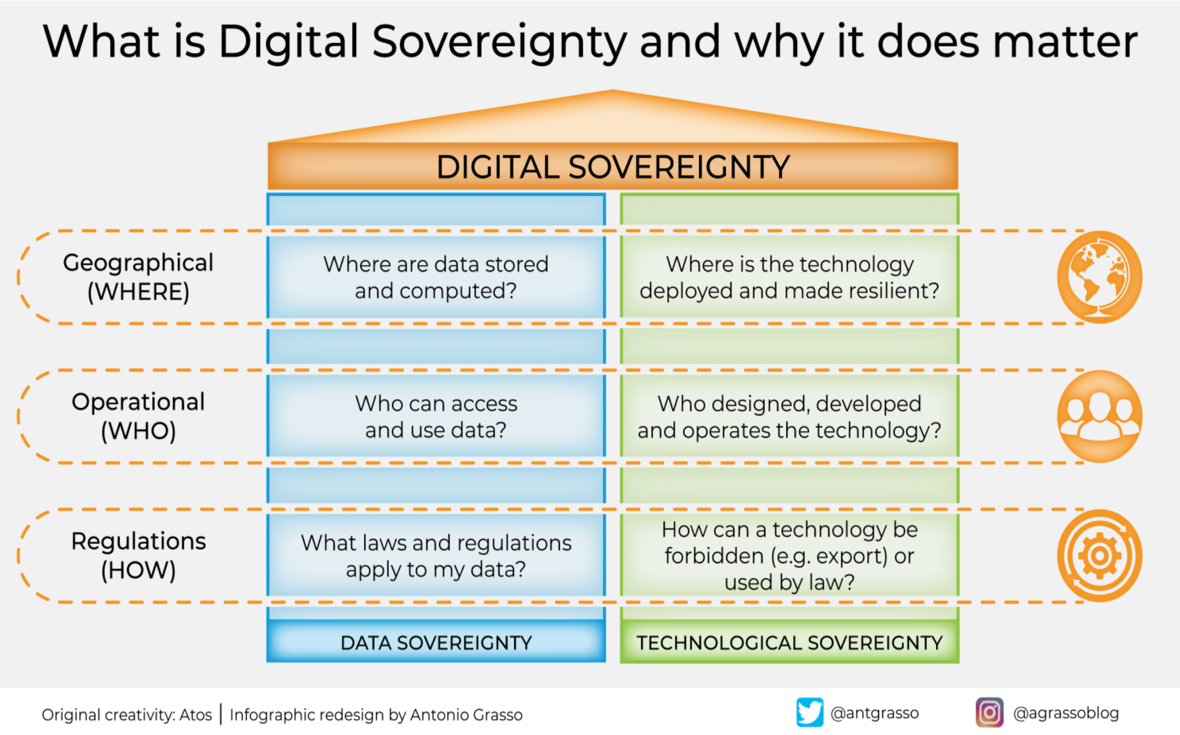
[4] Tietoevry.com, “Digital Sovereignty - What, Why and How?,” n.d., https://www.tietoevry.com/en/blog/2023/05/all-you-need-to-know-about-digital-sovereignty/.

Chinese companies like Huawei and TikTok are examples of actions taken to protect national security and digital sovereignty.

On September 29, 2021, the United States and the European Union's (EU) new Trade and Technology Council (TTC) held their first summit. It took place in the old industrial city of Pittsburgh, Pennsylvania, under the leadership of the European Commission's Vice-President, Margrethe Vestager, and U.S. Secretary of State Antony Blinken. Following the meeting, the U.S. and the EU declared their opposition to artificial intelligence (AI) that does not respect human rights and referenced rights-infringing systems, such as social scoring systems. During the meeting, the TTC clarified that "The United States and European Union have significant concerns that authoritarian governments are piloting social scoring systems with an aim to implement social control at scale. These systems pose threats to fundamental freedoms and the rule of law, including through silencing speech, punishing peaceful assembly and other expressive activities, and reinforcing arbitrary or unlawful surveillance systems." [5]

The U.S. and the EU's joint declaration against AI systems that do not respect human rights has led to stronger commitments to ethical AI development. Both sides have worked on establishing common frameworks and guidelines to ensure that AI technologies are developed and deployed in ways that uphold fundamental rights and freedoms. Increased global competition for technological leadership has led countries to view digital capabilities as a key source of economic and national security advantage.

[5] U.S.-E.U. Trade and Technology Council. "US-EU Trade and Technology Council Inaugural Joint Statement." White House Briefing Room Statements and Releases. September 29, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/



What is Digital Sovereignty and why it does matter

DIGITAL SOVEREIGNTY

	DATA SOVEREIGNTY	TECHNOLOGICAL SOVEREIGNTY
Geographical (WHERE)	Where are data stored and computed?	Where is the technology deployed and made resilient?
Operational (WHO)	Who can access and use data?	Who designed, developed and operates the technology?
Regulations (HOW)	What laws and regulations apply to my data?	How can a technology be forbidden (e.g. export) or used by law?

Original creativity: Atos | Infographic redesign by Antonio Grasso @antgrasso @agrassoblog

Source: Atos

The need to understand digital sovereignty

In an increasingly interconnected world, the concept of digital sovereignty has become a focal point for policymakers, businesses, and citizens alike. So the digital security professionals need to stay ahead of this complex but important concern. To ensure data security while leveraging the potential of AI, this is how countries can benefit from:

- Evaluating how their data will be used before investing in AI software and data-security solutions for government works.
- Regularly inspecting the nuts and bolts of their new and existing AI software for any vulnerabilities and risks.
- Leveraging trusted cybersecurity solutions to safeguard national and international business accounts and securely store sensitive information.[6]

[6] "Balancing Security and Innovation in the Age of AI | Bitwarden," Bitwarden, n.d., https://bitwarden.com/data-security-in-age-of-ai-mobile/.

By ensuring control over their own digital infrastructure and policies, countries can better protect their interests, foster innovation, and contribute to a more secure and equitable digital world. Understanding digital sovereignty is essential for several reasons, because by ensuring control over data and technological infrastructure, nations can protect their interests, including national security, economic stability, data privacy, and the promotion of democratic values.

- **National Security:** Protecting critical digital infrastructure is essential to prevent cyberattacks that can disrupt vital services and cause significant harm. Ensuring digital sovereignty helps safeguard communication networks, power grids, and financial systems from external threats. Additionally, reducing dependence on foreign technologies mitigates risks associated with geopolitical tensions and espionage, enhancing overall national security. [7]
- **Economic Stability:** Promoting domestic tech industries stimulates innovation, job creation, and economic growth, particularly in emerging fields like artificial intelligence and biotechnology. By investing in local research and development, countries can reduce reliance on foreign technology and boost their economic resilience.[8] A strong regulatory framework that aligns with digital sovereignty principles helps ensure fair competition, preventing monopolistic practices and protecting smaller enterprises.
- **Data Privacy and Protection:** Controlling personal data storage and processing within the country helps safeguard citizens' privacy and prevent data misuse. Ensuring that data is subject to local laws builds trust in digital services and protects sensitive information. Compliance with data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), ensures that citizens' rights are upheld and that personal data is handled responsibly.[9]

[7] Internet Society, “Navigating Digital Sovereignty and Its Impact on the Internet,” December 15, 2023, https://www.internetsociety.org/resources/doc/2022/navigating-digital-sovereignty-and-its-impact-on-the-internet/.

[8] Agathe Nageotte, “Digital Sovereignty and Economic Growth,” Oodrive, August 29, 2023, https://www.oodrive.com/blog/regulation/digital-sovereignty-and-economic-growth/

[9] Agathe Nageotte, “Digital Sovereignty and Economic Growth,” Oodrive, August 29, 2023, https://www.oodrive.com/blog/regulation/digital-sovereignty-and-economic-growth/.

- **Promotion of Democratic Values:** Digital sovereignty enables democratic countries to resist authoritarian practices like mass surveillance and social scoring systems. By controlling their own digital infrastructure, these nations can ensure that technology is used to enhance, rather than undermine, democratic values.[10] Additionally, protecting freedom of expression online by setting local content moderation and digital governance rules prevents censorship and supports an open exchange of ideas.
- **Global Influence and Leadership:** Prioritizing digital sovereignty allows countries to play a leading role in shaping global standards and norms for digital governance. By promoting ethical practices and human rights in the digital realm, they can influence international policies and agreements. Having control over their own digital assets enables countries to engage more effectively in international collaborations on cybersecurity, data protection, and technology development, strengthening global partnerships.[11]

Source: The 360 blog

[10] Rahel Süß, "Who Is the Digital Sovereign?," *Democratic Theory* 10, no. 2 (December 1, 2023): 56–66, https://doi.org/10.3167/dt.2023.100206.

[11] Benjamin Cedric Larsen, "The Geopolitics of AI and the Rise of Digital Sovereignty," Brookings, December 8, 2022, https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.

The Challenges of Digital Independence

Navigating digital sovereignty can pose challenges for many organizations, but there are answers for every top concern. And for good measure, organizations should remain flexible and adjust their approaches as the data and security landscape evolves.[12]

A primary challenge is technological dependency, as many countries rely heavily on foreign technology providers for hardware, software, and services. Reducing this dependency requires substantial investment in domestic research and development, infrastructure, and talent, which is both costly and time-consuming.[13] Economic constraints further complicate efforts to attain digital sovereignty. Building a self-sufficient digital infrastructure and fostering domestic tech industries necessitate significant financial resources. Countries with limited economic capabilities may struggle to make these investments, and ensuring fair competition in the digital market requires robust regulatory frameworks that are challenging to implement and enforce. [14]

Regulatory and legal challenges are also significant. Developing comprehensive frameworks for data protection, cybersecurity, and digital governance involves balancing regulation with innovation and growth. Achieving compliance with international standards while maintaining national sovereignty is a delicate task that requires careful policymaking. [15] A skilled workforce is essential for digital sovereignty, yet many nations face shortages in key areas like artificial intelligence and cybersecurity. Investing in education and training to build a talent pipeline is crucial but requires substantial time and resources.

Cybersecurity threats pose another major challenge. Protecting digital infrastructure from increasingly sophisticated cyberattacks necessitates continuous investment in robust cybersecurity measures and adaptability to evolving threats. International cooperation is often necessary to tackle global challenges such as cybersecurity and data protection. Balancing the need for cooperation

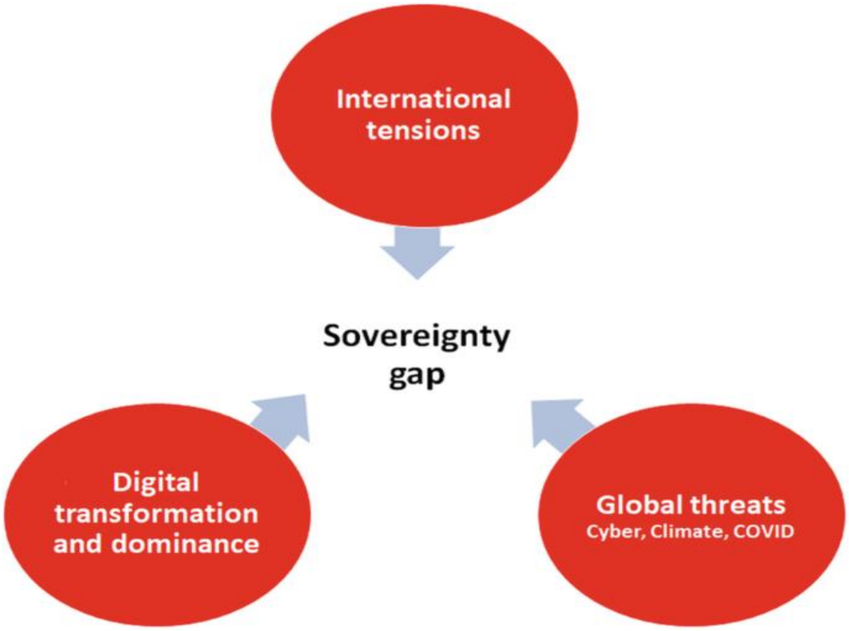
[12] Marg Pascucci and Matthew Parin, "Customer Trust Is Everything — Here'S How to Protect It With Digital Sovereignty," Salesforce, May 23, 2024, https://www.salesforce.com/blog/digital-sovereignty/.

[13] Pascucci and Parin, "Customer Trust Is Everything — Here'S How to Protect It With Digital Sovereignty."

[14] Oodrive Team, "Digital Sovereignty and Its Challenges: The Keys to Your Full Understanding," Oodrive, November 8, 2023, https://www.oodrive.com/blog/actuality/digital-sovereignty-keys-full-understanding/.

[15] Antonio Grasso, "Digital Sovereignty: What It Means and Why Governments Consider Data and Digital Technologies Strategic Infrastructure," December 5, 2022, https://www.linkedin.com/pulse/digital-sovereignty-what-means-why-governments-consider-grasso/.

with the pursuit of sovereignty can be difficult, particularly in a competitive global landscape where technological leadership is highly sought after.[16]



Source: SpringerLink

Collaboration between the public and private sectors is vital but can be challenging to achieve. Governments must create conditions conducive to innovation while ensuring compliance with national regulations.[17] Additionally, ethical considerations, such as data privacy and algorithmic bias, must be addressed to foster public trust in digital governance.

Conclusion

In the digital age, achieving digital sovereignty is imperative for nations to safeguard their national security, economic stability, and democratic values. This endeavor involves significant challenges, such as reducing dependency on foreign technologies, addressing economic constraints, and

[16] Oodrive Team, “Digital Sovereignty and Its Challenges: The Keys to Your Full Understanding,” Oodrive, November 8, 2023, https://www.oodrive.com/blog/actuality/digital-sovereignty-keys-full-understanding/.

[17] Marg Pascucci and Matthew Parin, “Customer Trust Is Everything — Here’S How to Protect It With Digital Sovereignty,” Salesforce, May 23, 2024, https://www.salesforce.com/blog/digital-sovereignty/.

developing robust regulatory frameworks. Nations must also invest in education to build a skilled workforce capable of driving innovation in critical areas like AI and cybersecurity. Furthermore, protecting digital infrastructure from sophisticated cyberattacks requires continuous investment in advanced cybersecurity measures.

Balancing international cooperation with the pursuit of sovereignty is another critical challenge, especially in a competitive global landscape. Effective collaboration between the public and private sectors is essential to foster innovation while ensuring compliance with national regulations and ethical standards. By addressing these challenges, countries can better control their digital infrastructure, protect personal data, and promote fair competition.

Ultimately, prioritizing digital sovereignty enables nations to shape global standards for ethical digital governance and human rights, thereby enhancing their global influence. Understanding and implementing digital sovereignty is crucial for countries to protect their interests, foster innovation, and contribute to a secure, equitable digital world. By navigating these complexities, nations can ensure their digital future is resilient, independent, and aligned with their core values.