

Article Information

Received: 15 Mar 2026

Revised: 14 May 2026

Accepted: 12 Jun 2026

Published: 30 Jun 2026

Original Article

The Sovereign Data Frontier: National Security, Digital Rights, and the Future of International Cyber Law

Nithil Fernandopulle¹

Author to whom any correspondence is to be addressed.

e-mail: nithilfernandopulle@gmail.com

Keywords: Data Sovereignty, Digital Rights, International Cyber Law, Extraterritorial Jurisdiction

Abstract

The digital age has precipitated a fundamental reconfiguration of sovereignty, shifting the locus of state authority from territorial borders to the governance of data. This article examines the emergent concept of data sovereignty as a critical flashpoint in international law, analyzing the tensions between states' national security imperatives, individual digital rights, and the imperative for a globally interoperable cyberspace. Through an examination of key legal instruments—including the EU's General Data Protection Regulation, the U.S. CLOUD Act, and China's Personal Information Protection Law—and seminal cases such as Microsoft Ireland, this paper maps the fragmented landscape of contemporary data governance. It argues that the current trajectory toward "Internet Balkanization" poses significant risks to both fundamental rights and global digital cooperation. The article proposes a normative framework for international cyber law anchored in principles of proportionality, due diligence, and a functional approach to jurisdiction that transcends physical borders while respecting legitimate sovereign interests.

Introduction

The concept of sovereignty, rooted in the Peace of Westphalia (1648), has traditionally been defined by territorial integrity, supreme authority within borders, and non-

¹Attorney-at-Law, University of West London – United Kingdom

interference from external powers². In the twenty-first century, this paradigm is being fundamentally challenged by the intangible, borderless nature of cyberspace. As societies grow increasingly dependent on digital infrastructure for essential functions—from commerce and healthcare to governance and national security—the question of ‘who’ governs digital data has become as consequential as the question of ‘who’ governs territory³.

The "Sovereign Data Frontier" describes the dynamic and contested space where states seek to reassert control over data generated within or traversing their jurisdictions. This impulse toward digital sovereignty is propelled by a confluence of factors: revelations of mass surveillance, the geopolitical dominance of a few global technology corporations, escalating cyber threats, and the recognition of data as a strategic economic and security asset^{4,5}.

However, the assertion of state control clashes with the inherent architecture of the internet, which was designed for the frictionless flow of information. This creates profound legal dilemmas. Can the traditional rules of territorial jurisdiction apply effectively to data that exists in a "cloud" spanning multiple legal jurisdictions? How should international law balance a state's right to protect its citizens' data from foreign surveillance against the need for cross-border data flows that underpin the global economy? This article explores these questions by analyzing the evolution of data sovereignty, mapping the divergent legal frameworks that embody it, and proposing a path toward a more coherent and balanced international cyber law.

The Evolution of Sovereignty in Cyberspace

❖ From Territorial Borders to Digital Borders

The transformation of sovereignty in the digital age can be traced to the early 2010s, crystallized by the 2013 Edward Snowden disclosures. The revelations of widespread surveillance by the U.S. National Security Agency prompted nations, including

² M. Simelane, "Africa's data, the new sovereignty frontier," Southern Africa Litigation Centre, Mar. 2026.

³ "Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law," Computer Law & Security Review, vol. 58, 106180, Sep. 2025.

⁴ R. Shrivastava et al., "Securing Borders in Cyberspace: Quest for Data Sovereignty Amidst Global Trade, Human Rights and Cross-Border Privacy Concern," Lex localis - Journal of Local Self-Government, Oct. 2024.

⁵ "The political dimensions of digital sovereignty," Journal of Interdisciplinary Studies in Society, Law, and Politics, vol. 4, no. 2, pp. 219-233, 2025.

Germany and Brazil, to reconsider their reliance on U.S.-controlled digital infrastructure and to call for greater control over their digital domains^{6,7}. This marked a shift from viewing the internet as a "global commons" to recognizing it as a domain of strategic competition, sometimes referred to as "Internet Balkanization"—the fragmentation of the global internet along national lines⁸.

At its core, data sovereignty is the principle that data is subject to the laws and governance of the nation-state where it is collected or processed⁹. This concept has rapidly evolved from a technical privacy concern into a fundamental element of national security and geopolitical strategy. States increasingly view data not merely as an asset to be protected but as a component of national identity and political independence. As argued in the African context, "true sovereignty in the 21st century will belong to those who command their digital domain".

❖ The Competing Visions: Open Internet vs. State Control

A fundamental schism divides the international community's approach to cyberspace governance¹⁰. On one side, a coalition of Western states, led by the United States and members of the European Union, has historically championed a multi-stakeholder model of internet governance. This model emphasizes an open, global internet underpinned by cooperative principles and the participation of private actors, civil society, and governments in norm-setting^{11,12}. This perspective aligns with a liberal economic order and views the free flow of data as essential for innovation and economic growth.

Conversely, an opposing camp, prominently including China and Russia, advocates for a state-centric "cyber sovereignty" model. This approach prioritizes centralized

⁶ R. Shrivastava et al., "Securing Borders in Cyberspace: Quest for Data Sovereignty Amidst Global Trade, Human Rights and Cross-Border Privacy Concern," *Lex localis - Journal of Local Self-Government*, Oct. 2024.

⁷ Jinseong Heo, "Global Trend of Data Localization Policy and its Legal Implications," *KCI*, Aug. 2025.

⁸ *Id*

⁹ *Id*

¹⁰ A. Shokri, "Sovereignty in Cyberspace from the Viewpoint of International Law," *Asian Journal of International Law*, Oct. 2025.

¹¹ "Sovereignty in Cyberspace from the Viewpoint of International Law," **Asian Journal of International Law**, Oct. 2025.

¹² "The political dimensions of digital sovereignty," *Journal of Interdisciplinary Studies in Society, Law, and Politics*, vol. 4, no. 2, pp. 219-233, 2025.

state control, surveillance capabilities, and national resilience. It views sovereignty as the unilateral capacity of a government to impose rules on all digital activities within its borders, irrespective of global implications, and often involves censorship, data localization, and strict restrictions on cross-border data flows. This divergence is not merely a technical disagreement but reflects deeper ideological chasms regarding the role of the state versus the individual in the digital sphere.

The Legal Architecture of Data Sovereignty

❖ Domestic Frameworks: The Triad of Power

The abstract concept of digital sovereignty is given concrete expression through domestic legislation. Three dominant regulatory models—embodied by the European Union, the United States, and China—represent the primary legal architectures shaping global data governance.

❖ The European Union: Rights-Based Model

The EU's General Data Protection Regulation (GDPR), effective since 2018, is the paradigmatic example of a rights-based approach. The GDPR enshrines privacy as a fundamental human right, imposing stringent requirements on the collection, processing, and transfer of personal data¹³. Its hallmark is its extraterritorial reach, applying to any organization, anywhere in the world, that processes the data of EU residents. Cross-border data transfers are permitted only if "adequate safeguards" are in place, such as a formal adequacy decision from the European Commission or Standard Contractual Clauses¹⁴. The GDPR sets a high global standard and has inspired similar legislation worldwide.

❖ The United States: Security and Access Model

In contrast to the EU's comprehensive framework, the U.S. employs a more sectoral and security-oriented approach. The Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 allows U.S. law enforcement to compel domestic technology companies to produce data stored overseas, regardless of the data's physical

¹³ "A Stage with Three Kings: EdTech, Sovereignty, and the Future of Transatlantic Data Law," Washington University Law Review, Jan. 2026.

¹⁴ "The political dimensions of digital sovereignty," Journal of Interdisciplinary Studies in Society, Law, and Politics, vol. 4, no. 2, pp. 219-233, 2025.

location¹⁵. This represents a powerful assertion of extraterritorial jurisdiction, prioritizing law enforcement access over the privacy frameworks of other nations. The CLOUD Act also facilitates bilateral "executive agreements" with allied nations to streamline data access for criminal investigations, further shaping the global landscape of data access.

❖ **China: State-Centric Sovereignty**

China's legal framework exemplifies the state-centric model. This is realized through a trilogy of laws: the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law (PIPL). These laws mandate strict data localization for certain categories of "important" or "sensitive" data, requiring it to be stored and processed within China. International data transfers are subject to rigorous government security assessments. The Chinese model is designed to maximize state control over data as a tool for national security, economic planning, and social governance, reflecting a collectivist ethos where individual rights are subsumed within state-defined societal interests¹⁶.

❖ **The Clash of Norms: Jurisdictional Conflict**

The coexistence of these divergent legal frameworks creates significant conflict. The case of *Microsoft Ireland* is a seminal illustration. In this dispute, U.S. authorities sought to compel Microsoft to produce emails stored on a server in Dublin, Ireland, for a criminal investigation. Microsoft resisted, arguing that U.S. courts lacked jurisdiction over data stored on foreign soil. The case, which involved over 289 groups from 37 countries supporting Microsoft's position, exposed the fundamental tension between the borderless nature of cloud computing and territorially bounded legal authority. The CLOUD Act was subsequently enacted in part to resolve this issue by codifying the U.S. government's ability to compel data access regardless of location—a move that directly challenges the sovereignty of other nations.

This jurisdictional conflict is a key source of contemporary legal tension. When an EdTech company based in the U.S. stores student data in Europe, it is subject to both U.S. law enforcement requests under the CLOUD Act and the EU's GDPR restrictions on data access and transfer. This creates a compliance nightmare for

¹⁵ "The political dimensions of digital sovereignty," *Journal of Interdisciplinary Studies in Society, Law, and Politics*, vol. 4, no. 2, pp. 219-233, 2025.

¹⁶ *Id*

businesses and intensifies the geopolitical struggle over who ultimately controls global data flows. The current situation is often described as a "fragmented" legal landscape where outdated international instruments like Mutual Legal Assistance Treaties (MLATs) are too slow and cumbersome to address the speed of modern digital investigations.

The Geopolitical Battlefield: Cyberspace, Security, and National Rights

❖ Cybersecurity as a Geopolitical Tool

The struggle for data sovereignty is intrinsically linked to cybersecurity, which has become a primary tool of geopolitical rivalry¹⁷. State-sponsored cyber operations target critical infrastructure, intellectual property, and sensitive government data. The attribution of these attacks is often difficult, creating a sense of impunity and emboldening malicious actors. In response, states assert greater control over their digital ecosystems, viewing it as a necessary defense against foreign interference. This dynamic has led to a "cyber arms race" where nations invest heavily in both offensive and defensive capabilities, further fragmenting the digital landscape.

❖ Digital Colonialism and the Global South

For nations in the Global South, the issue of data sovereignty carries the added weight of post-colonial history. Concerns about "digital colonialism" highlight the power imbalance where data from developing nations is extracted, processed, and monetized by foreign tech giants, primarily based in the U.S. or China¹⁸. This not only represents an economic loss but also raises concerns about cultural manipulation, political influence, and the erosion of national autonomy. The African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) is an attempt to assert continental data sovereignty, but its implementation is hampered by limited resources and technological capacity. These nations find themselves in a vulnerable position, seeking to attract foreign investment in digital infrastructure while fearing the loss of control over their citizens' data.

❖ Technology Companies as Sovereign Actors

¹⁷ "Cybersecurity as a Geopolitical Battlefield: Threats to National Sovereignty," Zenodo, Apr. 2025.

¹⁸ M. Simelane, "Africa's data, the new sovereignty frontier," Southern Africa Litigation Centre, Mar. 2026. <https://www.southernafricalitigationcentre.org/africas-data-the-new-sovereignty-frontier/>

The debate over data sovereignty also forces a reckoning with the role of private technology corporations, which have emerged as powerful non-state actors. Companies like Google, Amazon, and Microsoft are not merely intermediaries but are themselves sovereign-like entities that possess immense influence over the global digital ecosystem. Through their technical architectures, terms of service, and lobbying power, they shape the *de facto* rules of data governance. The challenge for international law is to account for these transnational private actors alongside traditional state-centric models, creating a need for new theories of accountability and jurisdiction that include corporate responsibility¹⁹.

The Way Forward: Forging a New International Cyber Law

❖ The Fragmented Lex Cyberia

The current state of international cyber law is often described as "fragmented," "outdated," and "incoherent". There is no universally accepted definition of a "cyberattack" or "cyberwarfare," and the applicability of fundamental principles like non-intervention and self-defense to cyberspace remains contested. The primary multilateral efforts, such as the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), have only succeeded in agreeing upon non-binding norms of responsible state behavior, and their work is often hampered by the geopolitical tensions between the major powers. The Tallinn Manual, while a monumental effort by international legal experts to clarify the application of existing law to cyber operations, remains a non-binding academic exercise^{20,21}.

❖ A Normative Framework for the Sovereign Data Frontier

In navigating this complex legal terrain, this article proposes a normative framework to guide the evolution of international cyber law. This framework rests on three key principles:

Proportionality and Necessity: States' assertions of digital sovereignty, particularly through data localization mandates and surveillance, must be subject to a test of proportionality and necessity. Measures must be strictly tailored to

¹⁹ Id

²⁰ M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, 2017.

²¹ "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," National Security Archive, Apr. 2019.

achieve a legitimate public policy objective (e.g., national security, consumer protection) and must not be more restrictive than necessary. This principle, drawn from both human rights law and international trade law, would provide a standard to evaluate the legality of excessive localization laws.

A Functional Approach to Jurisdiction: The traditional territorial model of jurisdiction is ill-suited to the cloud. A functional approach would determine jurisdiction based on the nature of the activity and its "significant effects" on a state, rather than solely on the data's physical location. The Functional Equivalent of the Border concept proposes that states can exercise jurisdiction over data if the data processor's activities produce a material and foreseeable effect within its territory. This would allow states to protect their interests without requiring the physical localization of data.

Due Diligence and State Responsibility: The international legal principle of due diligence requires states to ensure that territory under their control is not used to harm other states. This principle should be applied proactively to cyberspace. States must be responsible for preventing cyber operations launched from their territory that cause significant harm to another state, regardless of whether the attackers are state or non-state actors. Establishing effective mechanisms for international cooperation and attribution would reinforce this principle.

By anchoring future legal developments in these principles, the international community can move beyond the current stalemate. Instead of a unilateral race for control, a framework of mutual respect, shared obligations, and clear jurisdictional rules could help stabilize cyberspace, protect both national security and individual rights, and preserve the benefits of a globally connected digital economy.

Conclusion

The Sovereign Data Frontier is the central legal and political battleground of the twenty-first century. The assertion of data sovereignty represents a fundamental shift in the nature of state power, as nations seek to govern their digital domains in an era of unprecedented connectivity. The conflict between national security, digital rights, and the imperative for global digital cooperation is not a zero-sum game. A fragmented cyberspace, characterized by isolated national "digital walls," would ultimately harm all states—stifling innovation, undermining economic growth, and

exacerbating the very security risks it seeks to mitigate. The future of international cyber law will depend on a delicate and pragmatic balance. It must acknowledge the legitimate sovereignty of states while developing functional, adaptable legal norms that respect the rights of individuals and the realities of a borderless digital world. The task is to build a "lex cyberia" that is not merely a collection of competing national laws, but a coherent and just international framework for the digital age.

Bibliography

R. Shrivastava et al., "Securing Borders in Cyberspace: Quest for Data Sovereignty Amidst Global Trade, Human Rights and Cross-Border Privacy Concern," *Lex localis - Journal of Local Self-Government*, Oct. 2024. <https://lex-localis.org/index.php/LexLocalis/article/view/802499>

"A Stage with Three Kings: EdTech, Sovereignty, and the Future of Transatlantic Data Law," *Washington University Law Review*, Jan. 2026. <https://wustllawreview.org/2026/01/12/a-stage-with-three-kings-edtech-sovereignty-and-the-future-of-transatlantic-data-law/#post-24503-footnote-ref-129>

"Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law," *Computer Law & Security Review*, vol. 58, 106180, Sep. 2025. <https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000537>

Jinseong Heo, "Global Trend of Data Localization Policy and its Legal Implications," *KCI*, Aug. 2025. <https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artId=ART001942066>

M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, 2017. <https://link.europarl.europa.eu/portal/AHtRICrV52k>

M. Simelane, "Africa's data, the new sovereignty frontier," *Southern Africa Litigation Centre*, Mar. 2026. <https://www.southernafricalitigationcentre.org/africas-data-the-new-sovereignty-frontier/>

"Sovereignty in Cyberspace from the Viewpoint of International Law," **Asian Journal of International Law**, Oct. 2025. <https://www.cambridge.org/core/journals/asian-journal-of-international-law/article/abs/sovereignty-in-cyberspace-from-the-viewpoint-of-international-law/2193733BFBA268E7E211FA345942150>

"The political dimensions of digital sovereignty," *Journal of Interdisciplinary Studies in Society, Law, and Politics*, vol. 4, no. 2, pp. 219-233, 2025. <https://www.journalisslp.com/index.php/isslp/article/download/309/516/1730#4#2>

M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, 2017. <https://www.cambridge.org/mv/universitypress/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=HB&isbn=9781107177222>

S. Fatima, "Data Sovereignty vs Data Globalization: Legal Dilemmas in an Era of Digital Borders and Borderless Data," *International Journal of Law Management & Humanities*, May 2025.

A. Shokri, "Sovereignty in Cyberspace from the Viewpoint of International Law," *Asian Journal of International Law*, Oct. 2025. <https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Ashkan+SHOKRI&eventCode=SE-AU>
"Digital sovereignty, sovereign clouds and data embassies," *International Bar Association*, 2026.

"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," *National Security Archive*, Apr. 2019. <https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations>

M. I. Ali, "From Sovereignty to Surveillance: The Legal Landscape of 'Digital Colonialism' in India and Pakistan," *Paradigm*, May 2025.

"Cybersecurity as a Geopolitical Battlefield: Threats to National Sovereignty," *Zenodo*, Apr. 2025. <https://zenodo.org/records/15317864>

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

• **Conflict of Interest:** NIL

• **Funding Sources:** NIL
