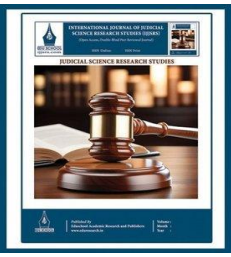
INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: 3049-0618 ISSN Print: 3108-2785



Data Sovereignty And International Legal Frameworks: Challenges Ahead

Nikhil Biju

LLM Student, Symbiosis Law school , Pune, India.

Article information

Received: 6th February 2026
Received in revised form: 8th March 2026
Accepted: 12th April 2026
Available online: 21st May 2026

Volume: 3
Issue: 2
DOI: https://doi.org/10.5281/zenodo.20036366

Abstract

Data sovereignty has emerged as a critical legal and policy challenge in the digital age, raising fundamental questions about territorial jurisdiction, cross-border data flows, and state authority over information resources. This paper examines the complex interplay between national data sovereignty claims and the international legal frameworks governing digital commerce and human rights. Through critical analysis of regional regulatory divergence particularly between the European Union's General Data Protection Regulation, China's data localization requirements, and fragmented approaches in other jurisdictions this study identifies three principal challenges: jurisdictional conflicts in extraterritorial data governance, tensions between economic integration and sovereignty claims, and inadequacies in existing international legal mechanisms. The analysis reveals that current frameworks, rooted in pre-digital conceptions of territoriality, struggle to accommodate the borderless nature of data flows while respecting legitimate sovereignty interests. This paper argues that addressing these challenges requires developing new international legal principles that balance state sovereignty with global connectivity, protect fundamental rights across borders, and establish enforceable mechanisms for cross-border cooperation. The findings contribute to ongoing debates about digital governance and highlight the urgent need for harmonized international standards.

Keywords: - Data Sovereignty, Extraterritorial Jurisdiction, Cross-Border Data Flows, Data Localization, GDPR, Law

I. INTRODUCTION

The exponential growth of digital data and its transnational flow has fundamentally challenged traditional notions of territorial sovereignty and jurisdictional authority. Data sovereignty the principle that data is subject to the laws and governance structures of the nation where it is collected or resides has become a central concern for states seeking to assert control over digital information within their borders (Irion, 2012). This concept intersects with complex international legal frameworks governing trade, privacy, security, and human rights, creating what scholars have termed a "regulatory patchwork" that both enables and constrains state action in the digital realm (Chander & Lê, 2015).

The emergence of data sovereignty as a legal priority reflects broader anxieties about technological power, economic competition, and national security in an increasingly digitized global economy. States across different regions have responded with divergent regulatory strategies, from the European Union's rights-based approach emphasizing data protection and privacy to authoritarian models prioritizing state access and control (Bradford, 2020). These competing visions have created significant tensions within international legal frameworks designed for an earlier era of globalization.

This paper examines three interrelated challenges facing international legal frameworks in addressing data sovereignty: jurisdictional conflicts arising from extraterritorial data governance, tensions between economic integration and sovereignty assertions, and the inadequacy of existing international legal mechanisms. Understanding these challenges is essential for developing effective legal responses that can accommodate legitimate state interests while preserving the benefits of digital connectivity and protecting fundamental rights. The analysis draws on comparative legal scholarship, international law theory, and empirical evidence of regulatory conflicts to illuminate pathways toward more coherent international governance of data sovereignty.

II. THEORETICAL FRAMEWORK

2.1. Sovereignty in the Digital Age

Classical theories of sovereignty, rooted in the Westphalian system, conceive of state authority as territorially bounded and mutually exclusive (Krasner, 1999). However, digital data flows challenge this territorial model by enabling information to traverse borders instantaneously and reside simultaneously in multiple jurisdictions. This deterritorialization of information has prompted scholars to reconceptualize sovereignty in functional rather than purely territorial terms (Sassen, 2008). Data sovereignty represents an attempt to reassert territorial control over what is inherently non-territorial, creating inherent tensions that international legal frameworks must address.

The concept of "digital sovereignty" extends beyond data to encompass broader questions of autonomy in the digital sphere, including control over critical infrastructure, technological standards, and platform governance (Pohle & Thiel, 2020). This expanded conception reflects recognition that data governance implicates fundamental questions about political authority, economic power, and cultural autonomy in the twenty-first century. Different states have articulated divergent visions of digital sovereignty, shaped by their political systems, economic positions, and cultural values.

2.2. Jurisdictional Theory and Extraterritoriality

International law traditionally recognizes three bases for jurisdiction: territorial, nationality, and protective (Restatement Third of Foreign Relations Law, 1987). Data governance regulations increasingly invoke all three bases, often simultaneously, creating complex jurisdictional overlaps. The European Union's GDPR exemplifies this trend through its assertion of jurisdiction over any processing of EU residents' data, regardless of where that processing occurs or the processor's location (Kuner, 2017). This extraterritorial reach represents a significant departure from traditional territorial limitations on regulatory authority.

Scholarly debate continues regarding the legitimacy and limits of such extraterritorial assertions. Some scholars defend expansive jurisdiction as necessary to protect rights in an interconnected world (Scott, 2014), while others caution that competing extraterritorial claims risk creating unworkable regulatory conflicts and undermining international comity (Swire & Bermann, 2007). This theoretical tension manifests in practical conflicts as states assert overlapping and sometimes contradictory jurisdictional claims over the same data flows.

III. ANALYSIS OF KEY CHALLENGES

3.1. Challenge One: Jurisdictional Conflicts and Extraterritorial Regulation

The first major challenge facing international legal frameworks is the proliferation of conflicting jurisdictional claims over data. The GDPR's extraterritorial application has created what scholars term the "Brussels Effect," whereby EU standards become de facto global standards due to the impracticality of maintaining different data practices for different jurisdictions (Bradford, 2020). However, this dynamic has generated significant tension with other jurisdictions asserting competing sovereignty claims.

The conflict between the GDPR and the U.S. CLOUD Act exemplifies these tensions. While the GDPR restricts transfers of personal data outside the EU without adequate protections, the CLOUD Act empowers U.S. law enforcement to compel U.S.-based service providers to produce data regardless of where it is stored (Daskal, 2018). Companies caught between these competing mandates face the prospect of violating one legal system regardless of their actions a situation that exposes the inadequacy of traditional conflict-of-laws principles for addressing digital governance.

Similarly, China's Cybersecurity Law and Data Security Law impose extensive data localization requirements and mandate government access to data, creating direct conflicts with privacy-protective regimes elsewhere (Creemers, 2022). These requirements reflect a fundamentally different conception of the relationship between individuals, data, and state authority. The result is a fragmented global data governance landscape where compliance with one jurisdiction's requirements may necessitate violation of another's, creating legal uncertainty for multinational entities and potentially fragmenting the internet along jurisdictional lines.

3.2. Challenge Two: Economic Integration Versus Sovereignty Claims

International economic law has long prioritized free flow of information and data as essential to trade and economic integration. The General Agreement on Trade in Services (GATS) and various free trade agreements contain provisions limiting restrictions on cross-border data transfers (Burri, 2017). However, data sovereignty assertions increasingly conflict with these commitments, raising questions about the relationship between trade liberalization and regulatory autonomy.

The tension manifests acutely in disputes over data localization requirements, which mandate that certain data be stored or processed within a state's territory. Proponents justify such requirements on grounds of privacy protection, national security, law enforcement access, and economic development all recognized as legitimate regulatory objectives under international trade law (Casalini & López González, 2019). However, critics argue that many localization measures serve protectionist purposes or reflect authoritarian control rather than legitimate policy goals, and that they impose significant costs by fragmenting global digital services.

Recent trade agreements have attempted to address this tension through provisions prohibiting unjustified data localization while preserving policy space for legitimate regulatory objectives. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), for instance, prohibits data localization requirements but includes exceptions for legitimate public policy objectives (Aaronson, 2019). However, the breadth of these exceptions and difficulties in distinguishing legitimate from protectionist measures leave substantial uncertainty about the actual constraints on sovereignty assertions.

3.3. Challenge Three: Inadequacy of Existing International Legal Mechanisms

Existing international legal mechanisms for addressing cross-border data governance prove inadequate for contemporary challenges. The primary multilateral framework the Council of Europe's Convention 108+ on data protection lacks universal membership and enforcement mechanisms (De Hert & Papakonstantinou, 2016). While it establishes important principles, its effectiveness is limited by its regional character and reliance on voluntary compliance.

Bilateral mechanisms, such as mutual legal assistance treaties (MLATs), provide formalized channels for cross-border data access but operate too slowly for the real-time needs of digital investigation and prove cumbersome for routine matters (Woods & Birnhack, 2023). The inadequacy of MLATs has driven unilateral assertions of extraterritorial jurisdiction, further exacerbating conflicts. Recent efforts to streamline cross-border access through the CLOUD Act's bilateral agreement mechanism represent promising developments but remain limited in scope and geographic coverage.

International human rights law provides important normative guidance through instruments like the International Covenant on Civil and Political Rights, which protects privacy as a fundamental right (Milanovic, 2011). However, the application of these protections to extraterritorial data access and the balancing of privacy against security and other state interests remain contested. Recent jurisprudence from the European Court of Human Rights has begun to address digital surveillance, but significant doctrinal uncertainty persists regarding the extraterritorial application of human rights obligations in the digital context.

3.4. Interpretation and Implications

The challenges identified above reveal a fundamental mismatch between the territorial logic of traditional international law and the deterritorialized reality of digital data flows. This mismatch generates three significant implications for international legal governance. First, absent coordinated international standards, regulatory fragmentation will likely intensify, potentially leading to the "Balkanization" of the internet as states impose incompatible requirements on data flows (DeNardis & Raymond, 2013). Such fragmentation would undermine the economic and social benefits of digital connectivity while failing to adequately protect the legitimate interests that drive sovereignty assertions.

Second, the proliferation of extraterritorial assertions creates compliance dilemmas for multinational entities and risks undermining respect for international legal principles more broadly. When compliance with one jurisdiction's laws requires violation of another's, the rule of law itself becomes attenuated. This situation threatens to erode norms of comity and cooperation that underpin international order, with potential spillover effects beyond data governance.

Third, inadequate international mechanisms leave fundamental rights protections vulnerable to the lowest common denominator. Without effective international safeguards, individuals' privacy and other digital rights depend entirely on the domestic laws of whichever jurisdiction proves most permissive or most powerful. This situation is particularly problematic given the global nature of digital services and the reality that data about individuals in one jurisdiction routinely transits through or is processed in jurisdictions with weaker protections.

3.5. Toward Coherent International Governance

Addressing these challenges requires developing new international legal frameworks that can accommodate the distinctive features of data governance while preserving core sovereignty interests and rights protections. Several scholars have proposed models for such frameworks, ranging from comprehensive multilateral treaties to sector-specific agreements and networked governance arrangements (Svantesson, 2020). While a detailed evaluation of these proposals exceeds this paper's scope, several principles emerge as essential for effective international data governance.

First, any effective framework must recognize legitimate diversity in national approaches while establishing baseline protections that apply across jurisdictions. The principle of "interoperability" rather than harmonization may prove more realistic and respectful of sovereignty, allowing different systems to interact effectively while maintaining their distinctive features (Greenleaf, 2012). Second, mechanisms for resolving jurisdictional conflicts must be formalized through clear rules of priority and procedures for cooperative resolution rather than unilateral assertion. Third, international governance structures must be genuinely multilateral, avoiding domination by either powerful states or economic actors.

Recent developments offer grounds for cautious optimism. The OECD's work on cross-border access to data for law enforcement, ongoing negotiations on e-commerce provisions in trade agreements, and regional initiatives like the African Union's data protection framework all represent steps toward more coherent international governance (Bygrave & Tosoni, 2020). However, these initiatives remain nascent, and significant political obstacles including great power competition and divergent ideological commitments complicate prospects for comprehensive agreement.

IV. CONCLUSION

Data sovereignty presents fundamental challenges to international legal frameworks developed for a pre-digital era. The tension between territorial jurisdiction and borderless data flows, competing assertions of extraterritorial authority, conflicts between economic integration and regulatory autonomy, and inadequate international mechanisms collectively threaten coherent governance of the digital realm. These challenges are not merely technical or administrative but implicate core questions about sovereignty, rights, and international order in the twenty-first century.

This analysis has demonstrated that current approaches whether unilateral extraterritorial assertions, bilateral agreements, or limited regional frameworks prove insufficient for addressing the scope and complexity of contemporary data governance challenges. The proliferation of conflicting national requirements creates legal uncertainty, imposes substantial compliance costs, threatens internet fragmentation, and leaves fundamental rights inadequately protected. Addressing these challenges requires developing international legal frameworks that can balance legitimate sovereignty interests with the practical and normative imperatives of global connectivity.

The path forward demands creative thinking about international governance mechanisms that can accommodate regulatory diversity while establishing enforceable baseline standards. Such mechanisms must address jurisdictional conflicts through clear rules and cooperative procedures, protect fundamental rights across borders, and provide effective enforcement while respecting sovereignty. While political obstacles remain formidable, the costs of continued fragmentation economic, social, and political make the development of more coherent international frameworks increasingly urgent. The challenge for international legal scholarship and practice is to develop governance structures adequate to the distinctive features of the digital age while preserving the core values that international law serves.

REFERENCES

Aaronson, S. A. (2019). Data is different, and that's why the world needs a new approach to governing cross-border data flows. *Digital Policy, Regulation and Governance, 21*(5), 441–460.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Burri, M. (2017). The regulation of data flows through trade agreements. *Georgetown Journal of International Law, 48*(1), 407–448.

Bygrave, L. A., & Tosoni, L. (2020). Article 45: Transfers on the basis of an adequacy decision. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 774–804). Oxford University Press.

Casalini, F., & López González, J. (2019). *Trade and cross-border data flows* (OECD Trade Policy Papers No. 220). OECD Publishing.

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal, 64*(3), 677–739.

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity, 8*(1), Article tyac011. https://doi.org/10.1093/cybsec/tyac011

Daskal, J. (2018). Borders and bits. *Vanderbilt Law Review, 71*(1), 179–240.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*(2), 179–194.

DeNardis, L., & Raymond, M. (2013). Thinking clearly about multistakeholder internet governance. *GigaNet: Global Internet Governance Academic Network Annual Symposium, 8*, 1–12.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108? *International Data Privacy Law, 2*(2), 68–92.

Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet, 4*(3–4), 40–71.

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.

Kuner, C. (2017). Reality and illusion in EU data transfer regulation post Schrems. *German Law Journal, 18*(4), 881–918.

Milanovic, M. (2011). *Extraterritorial application of human rights treaties: Law, principles, and policy*. Oxford University Press.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4), 1–19.

Restatement (Third) of Foreign Relations Law of the United States. (1987). American Law Institute.

Sassen, S. (2008). Neither global nor national: Novel assemblages of territory, authority and rights. *Ethics & Global Politics, 1*(1–2), 61–79.

Scott, J. (2014). Extraterritoriality and territorial extension in EU law. *American Journal of Comparative Law, 62*(1), 87–125.

Svantesson, D. J. B. (2020). *Solving the internet's legal problems: Privacy, data protection, and cybersecurity in the age of AI*. Edward Elgar Publishing.

Swire, P., & Bermann, D. (2007). Information privacy and jurisdictional conflicts: A case study of the European Union's General Data Protection Regulation. *International Data Privacy Law, 7*(4), 220–235.

Woods, A. K., & Birnhack, M. (2023). Extraterritorial surveillance and the clash of rights. *International Journal of Law and Information Technology, 31*(1), 1–45.