Sociology & Cultural Research Review (SCRR)
Available Online: https://scrrjournal.com
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

Digital Sovereignty or Global Integration? Pakistan's Data Governance in the Age of Transnational Law

Johar Wajahat
Assistant Professor, Department of Law, Shaheed benazir Bhutto women university Peshawar
johar.wajahat@sbbwu.edu.pk
Dr. Rafia Naz Ali
Assistant Professor, Department of Shariah and Law, Islamia College University Peshawar
rafia@icp.edu.pk
Arshad Nawaz Khan
Assistant Professor, School of Law, Quaid-i-Azam University, Islamabad
ankhan@qau.edu.pk

ABSTRACT
This research study has attempted to undertake a critical and in-depth examination of Pakistan's evolving data governance framework. The primary focus is the tension between the assertion of digital sovereignty and the requirements of global economic integration. The study challenges the prevailing policy reliance on technical legalism and data localization. It addresses a central paradox. This paradox is the persistence of significant data governance vulnerabilities despite the development of sophisticated proposed legislation like the Personal Data Protection Bill 2023. The analysis is grounded in a systematic assessment of functional legal and institutional failures. The findings reveal a fragmented regulatory environment. This environment is characterized by institutional overlaps and weak enforcement mechanisms. A nascent jurisdictional schism from provincial initiatives worsens the situation. The study concludes that effective governance requires moving beyond imitative legalism. It must instead pursue strategic harmonization with international standards. It must also build resilient domestic institutions. Achieving a balance between sovereign control and global participation is essential for a resilient digital economy.

Keywords: *Data Governance, Pakistan, Digital Sovereignty, Transnational Law, Cybersecurity, Data Localization, GDPR.*

Introduction

The global digital economy is defined by the seamless flow of data across national borders. This transnational movement of information supports modern communication and finance. It also supports trade. For developing states like Pakistan this connectivity presents a major opportunity for economic growth. It also presents a profound governance challenge. Pakistan has witnessed rapid digitalization. Rising internet penetration enables new forms of commerce and public service delivery. However, this integration into global data flows creates a core dilemma. This dilemma pits the desire for digital sovereignty against the economic necessity of global integration. Digital sovereignty means state control over data within its territory.

The current legal landscape in Pakistan remains fragmented. It consists of disparate instruments. These include the Prevention of Electronic Crimes Act 2016 and the outdated Electronic Transactions Ordinance 2002. The proposed Personal Data Protection Bill 2023 represents a concerted effort. It aims to establish a comprehensive and rights-based framework. This framework is inspired by international models like the European Union's

General Data Protection Regulation. Yet a significant paradox endures. Despite advancing legislative efforts systemic governance failures persist. These include institutional confusion and enforcement deficits. The unimpeded operation of multinational technology firms under minimal local accountability also continues.

This situation presents a central question for scholars and policymakers. The question is why profound data governance vulnerabilities persist. They persist despite increasingly rigorous laws designed to address them. Dominant policy analyses often focus on technical capacity gaps or cyber threat assessments. This focus can be critiqued as a form of digital fetishism. This fetishism prioritizes technical fixes and simplistic metrics. It overlooks a nuanced understanding of the institutional and political economy of enforcement. This paper moves beyond this limited lens. It conducts a systematic and comparative analysis. It analyzes the functional efficacy of Pakistan's data governance frameworks through the perspective of transnational law. The core argument posits that the governance deficit is not merely a product of absent legislation. It is rather a consequence of fundamental asymmetries. These asymmetries exist between sophisticated transnational legal standards and domestic institutional realities. The primary research inquiry is how the tensions between sovereign aspirations and integrationist needs manifest. They manifest in the failures and dilemmas of Pakistan's data governance strategy.

Literature Review: Beyond Techno Legalism and the Digital Trade Paradigm

Existing scholarly discourse on data governance in Pakistan is largely shaped by two paradigms. Each exhibits limitations for a holistic institutional analysis. The first is the techno legal and cybersecurity paradigm. This approach provides meticulous audits of legal provisions. It compares them to international benchmarks like the GDPR. It expertly identifies legislative gaps in areas such as data portability and purpose limitation. However, this paradigm often treats the state as a monolithic and rational actor. It explains what the law says but frequently fails to dissect procedural pathologies. It does not adequately analyze institutional conflicts and political pressures that determine how the law functions in practice. It advocates for an independent regulator. However, it may not analyze how provisions for governmental control undermine that independence from its inception.

The second paradigm is the political economy of digital trade and colonialism. This body of work examines global power asymmetries. These asymmetries enable multinational technology corporations to extract and monetize citizen data from the Global South. It highlights how international trade frameworks can perpetuate a form of digital dependency. This scholarship robustly explains structural incentives for weak local enforcement. It also explains external pressures shaping policy. However, it often engages at a macro level. It sometimes neglects a granular and procedural examination of the domestic legal machinery. It describes an environment of impunity. It less frequently traces how a specific case of data misuse fails due to admissibility rules or jurisdictional conflicts.

While these schools of thought effectively map the technical legal landscape they leave an analytical void. There is a deficit of micro level and institutional examination. This examination should focus on how data law is functionally implemented within the state apparatus. Furthermore, prevailing policy analysis can be susceptible to a compliance fetishism. This fetishism treats the passage of legislation as a sufficient metric of success. It overlooks the harder tasks of building resilient enforcement institutions. This article aims to address this critical gap. It shifts the analytical focus from the political economy of data flows to the political economy of data law enforcement. It provides a structured diagnosis of institutional performance and contradictions.

Theoretical Framework: Sovereignty, Integration, and the Transnational Legal Field

This study is situated within theoretical discourse on transnational law and digital sovereignty. Transnational law refers to legal rules and principles that transcend national borders. It encompasses hard law treaties and soft law standards like the GDPR. Digital sovereignty asserts a state's right to regulate the digital landscape within its territory. It often emphasizes control over data and infrastructure.

The theoretical tension explored here is between a Westphalian model of digital sovereignty and a networked model of global integration. The Westphalian model prioritizes territorial control. It often manifests in policies like data localization and stringent national security exemptions. This model is frequently motivated by security concerns and a desire for political autonomy. In contrast the networked model emphasizes interoperability and harmonized standards. It views the free flow of data as essential for economic innovation. This model is championed by economic blocs and multinational corporations.

Pakistan's data governance strategy represents an attempt to navigate these competing imperatives. However, this navigation is fraught with contradiction. The state seeks to project sovereign authority through comprehensive national legislation. It simultaneously needs to align with transnational standards to facilitate trade and investment. This creates a policy environment of aspirational convergence. It adopts the form of advanced data protection law without securing the functional prerequisites. The resultant dynamic is one of structural dissonance. Sophisticated laws are grafted onto an institutional landscape marked by fragmentation. This leads to a gap between legal promise and practical outcome.

Methodology

This study employs a qualitative comparative case study design. It is grounded in doctrinal legal analysis and policy assessment. The research philosophy is interpretivist. It focuses on the contextual meaning and functional application of legal texts within specific institutional settings. This approach is essential for understanding how key stakeholders interpret and operationalize data governance norms.

The research is based on the systematic analysis of primary legal and policy documents. This corpus includes Pakistan's Prevention of Electronic Crimes Act 2016. It also includes the draft Personal Data Protection Bill 2023 and the Digital Nation Pakistan Act 2025. Relevant rules and regulations and official policy statements are also analyzed. A particular focus is placed on tracing procedural requirements and institutional mandates. This primary analysis is supplemented by a critical review of secondary sources. These include academic literature and reports from international organizations. Analysis from civil society groups is also included. The comparative element is maintained through constant reference to the GDPR as a key benchmark.

Analysis I: The Architecture of Control: PECA 2016 and the Security Sovereignty Nexus

Pakistan's first major foray into comprehensive digital governance was the Prevention of Electronic Crimes Act 2016. This legislation primarily establishes a framework of digital sovereignty as control. Its overarching aim is to secure cyberspace against crime and terrorism. It also addresses threats to national security. In doing so it constructs a guardian oriented towards state security rather than individual data protection.

PECA creates broad offenses related to unauthorized access and data interference. It grants extensive investigative powers to the Federal Investigation Agency. These include the authority to seize data and require decryption. However, the Act has been widely criticized for its vague definitions. These definitions can be used to criminalize dissent. Furthermore, its

procedural safeguards are weak. While it mandates warrants for certain actions exceptions are broad. Oversight mechanisms are limited.

This security centric model creates a fundamental tension with a rights-based data protection regime. PECA positions the state as the primary guardian against digital threats. It also positions the state as a potent actor with sweeping surveillance capabilities. This poses a direct challenge to principles of purpose limitation and individual consent. The analysis reveals that Pakistan's data governance foundation is bifurcated. One pillar emphasizes sovereign control and security. The aspirational pillar seeks to establish privacy as a fundamental right. This unresolved tension within the legal architecture is a primary source of institutional confusion.

Analysis II: The Aspirational Framework: PDPB 2023 and the Mimicry of Transnational Standards

The Personal Data Protection Bill 2023 represents a deliberate effort to shift towards a model of digital sovereignty as rights-based governance. It is a legislative artifact of transnational legal influence. It directly mirrors core principles and structures of the GDPR. It establishes a National Commission for Personal Data Protection. It grants individuals rights like access and correction. It imposes obligations on data controllers and provides for restrictions on cross border data transfers.

A close doctrinal analysis however reveals critical deviations that undermine its aspirations. First the independence of the guardian is compromised. Unlike the GDPR's requirement for fully independent authorities the PDPB grants the federal government significant control. This control is over the appointment and budget of the commission. This creates a risk of political capture. Second expansive exemptions for state functions are embedded. The draft bill allows for processing of personal data without consent for vaguely defined reasons of national security. These exemptions are broader and subject to less judicial oversight than comparable provisions in the GDPR.

This analysis demonstrates a pattern of selective adoption. Pakistan adopts the GDPR's form while neutering its core enforcement mechanisms. It carves out substantial exceptions for state power. The result is a hybrid framework. It speaks the language of global integration and rights protection. However, it is architecturally designed to preserve sovereign state control in key areas. This creates a governance gap. Neither effective rights protection nor efficient global interoperability is fully achieved.

Analysis III: The Provincial Schism: Fragmentation of the National Legal Space

An emerging challenge to a unified data governance framework is the trend of provincial legislation. Following the 18th Amendment initiatives in Sindh and Punjab have proposed their own data protection laws. This development risks creating a jurisdictional schism within Pakistan's own legal space.

If provincial laws establish separate authorities or conflicting rules the result will be regulatory fragmentation. A multinational company operating across Pakistan would face a compliance nightmare. It would need to navigate multiple and potentially contradictory regimes. This internal fragmentation weakens Pakistan's position in transnational negotiations. It cannot argue for adequacy status from the EU with a fractured domestic landscape.

This provincial dynamic mirrors the tension between sovereignty and integration at a sub national level. Provincial governments assert their legislative sovereignty. In doing so they undermine the possibility of a strong and unified national framework. This framework is essential for effective global integration. It creates internal borders for data that exacerbate compliance costs and legal uncertainty.

Discussion: Navigating the Sovereignty Integration Dilemma

The analysis reveals that Pakistan's data governance strategy is trapped in a cycle of structural contradiction. It seeks the benefits of global integration by mimicking transnational standards. Yet it simultaneously insists on Westphalian sovereign controls. This is not a coherent strategy but a set of conflicting impulses.

The data localization debate epitomizes this dilemma. Mandating that certain data be stored domestically is a classic assertion of digital sovereignty. It is justified by security and economic arguments. However empirical evidence suggests such measures increase costs for local businesses. They hinder cloud adoption and provide questionable security benefits. They do little to prevent data extraction by platforms through other means. It is a sovereignty measure that actively impedes integration.

The pathway forward requires a move beyond symbolic legalism. Effective policy must bridge the internal governance gap. It must resolve the tension between different laws and prevent harmful provincial fragmentation. This necessitates clear legislative hierarchy and a genuinely independent commission with unified authority. Simultaneously Pakistan must pursue strategic interoperability externally. Instead of a binary choice it should advocate for interoperable regulations. These regulations should meet core privacy principles while allowing for pragmatic data flows. Engaging in coalitions of the Global South to shape international norms is a critical step.

Conclusion

Pakistan stands at a digital crossroads. The choice is not a simple binary between sovereignty and integration. The current path leads to a worst of both worlds' outcome. This path is characterized by aspirational but compromised legislation. It has internal institutional tensions and emerging fragmentation. The sophisticated legal architecture of the proposed bill is undermined by its own design flaws. It is also undermined by the unresolved dominance of the security state model.

True digital sovereignty in the 21st century is not achieved through isolation or legal mimicry alone. It is built on the foundation of effective internal governance. This requires robust institutions and credible rights protection. It also requires regulatory coherence. Only from a position of domestic strength can a state meaningfully engage in the transnational legal field. It can then negotiate terms of integration that protect its national interests. Therefore, Pakistan's immediate priority must be to consolidate its own digital governance framework. It must ensure it is unified and rights respecting. It must also ensure it is institutionally capable. From this foundation a pragmatic and sovereign engagement with global digital integration becomes possible.

References

Akhtar, N., & Yousaf, A. R. (2025). Cyber sovereignty: National security in the digital age. Lahore Institute for Research and Analysis Journal, 3, 87–104.

Ali, M. I., & Hussain, K. A. (2024). Unveiling the tapestry: A comparative investigation into data-protection legislation in India and Pakistan. Socrates, 28(1), 1–8.

Baloch, M. U. F. (2025). Importance of big data: Pakistan's struggle with big data governance. Policy Vanguard, 1(1).

Bhatti, A. B., & Afraz, T. (2025). Digital innovation, data, and rights: Reassessing Pakistan's intellectual property and cyber law framework. SSRN.

Chaudhry, P. (2023). The GDPR effect: How European data standards are shaping Pakistani law. Journal of International Data Privacy Law, 13(2), 89-104.

Firdous, N., Ashraf, M. U., Zia, S., & Ullah, I. (2025). Black box law: The crisis of transparency and legal accountability in algorithm-driven governance in Pakistan. Research Consortium Archive.
Fischer, A. (2023). Data sovereignty and e-governance: The legal implications of national laws on digital government systems. Legal Studies in Digital Age, 2(4), 1–12.
Halim, W., Upadhyay, A., & Coflan, C. (2022). Data access and protection laws in Pakistan: A technical review. EdTech Hub.
Jhokio, A., Rehman, T. U., & Kaleemullah. (2025). Data privacy laws in Pakistan: A comparative analysis with the EU's General Data Protection Regulation. Journal of Political Stability Archive, 3(2), 871–882.
Kaya, M., & Shahid, H. (2025). Cross-border data flows and digital sovereignty: Legal dilemmas in transnational governance. Interdisciplinary Studies in Society, Law, and Politics, 4(2), 219–233.
Kuzio, J., Ahmadi, M., Kim, K. C., Migaud, M. R., Wang, Y. F., & Bullock, J. (2022). Building better global data governance. Data & Policy, 4, e25.
Masudi, J. A., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age. Pakistan Journal of International Affairs, 6(3), 356–366.
Sohrab, L. B., Shah, K., & Nawaz, B. (2024). Bridging the gap: Cross-border data flows & data protection harmonization in Pakistan. Journal of Social Sciences Development, 3(3), 232–247.
Yanow, D., & Schwartz-Shea, P. (Eds.). (2015). Interpretation and method: Empirical research methods and the interpretive turn (2nd ed.). Routledge.
Yaseen, M. (2024). Cross-border data flows in Pakistan: Legal challenges and technological solutions for digital trade. Journal of Engineering, Science and Technological Trends, 1(1).
Zafar, U. B. (2025). Digital colonialism: Big Tech's impact on Pakistan and the Global South. UCP Journal of Law & Legal Education, 3(2), 29–55.