



Journal of Climate and Community Development

A Double-Blind, Peer-Reviewed, HEC recognized [Y-category](#) Research Journal

E-ISSN: [3006-7855](#) P-ISSN: [3006-7847](#)

Geopolitics of Data Sovereignty: Digital Borders and the Fragmentation of Global Order

Dr. Syed Shameel Ahmed Quadri¹ Rakhshanda Munir²

¹ Assistant Professor, Department of Political Science, University of Karachi, Sindh, Pakistan.

² Lecturer and Department Head of Political Science, DHACSS College for Women, Phase 8, Karachi, Sindh, Pakistan.

Corresponding Author: Dr. Syed Shameel Ahmed Quadri, **Correspondence through:** ishameel2007@gmail.com

Vol. 5, Issue 1, 2026

Article Information

Received:

2026-03-03

Revised:

2026-04-25

Accepted:

2026-06-20

ABSTRACT

This article examines the geopolitics of data sovereignty, the geopolitical rivalry among relevant state actors to assert regulatory authority over digital networks, the crossing of borders with data and the normative rules of the game in cyberspace. This research employs a comparative, qualitative and secondary data analysis method, which is in line with the most different systems design. The research explores different governance models implemented by the great powers such as United States, the European Union, and People's Republic of China, India and Russia and places each within the theoretical paradigms of weaponized interdependence, digital geopolitics, and the nexus of data, space, and power. The paper suggests that the global order is experiencing a real digital fragmentation, due to the interplay between different regulatory visions and rules of data localization, as well as diverging cybersecurity agendas, that are giving rise to a de facto splinternet, which is reflecting and exacerbating systemic tensions. The statistical evidence collected from various sources such as ITU, World Bank, UNCTAD, McKinsey Global Institute, Statista, OECD, Freedom House, IDC, Gartner, ECIPE and thirteen original comparative tables prove that Data Sovereignty is not just a technico-administrative question but has become a vital instrument of geopolitical power in the 21st century.

Keywords: *Data Sovereignty, Fragmentation of Global Order, Digital Geopolitics, Weaponized Interdependence, Brussels Effects, Digital Borders, Cyber Sovereignty, Regulatory Competition.*

Citation: APA

Quadri, S, S, A & Munir, R (2026). *Geopolitics of data sovereignty: Digital borders and the fragmentation of global order*, *Journal of Climate and Community Development*, 5(1), 217-235.



© 2026 by the authors. Licensee Quadri & Munir. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>

Introduction

Sovereignty has been regarded as the supreme and exclusive authority of the state over certain people and territory from the time of the Peace of Westphalia in 1648. Sovereignty is the foundation of the present international system for nearly 400 years. The Westphalia system established the state as the sovereign player in international politics, its borders sacrosanct, and its internal sovereignty supreme, its external sovereignty guaranteed by other sovereigns. But with the arrival of the 21st century, the system's architects face a challenge that they could never have envisioned. The new, fifth domain of geopolitics, cyberspace appeared in which sovereignty is not defined by artillery and treaties but by algorithms, data centers, regulatory architectures and the domination of undersea fiber optic cables. (Falencik, 2021; Budnitsky, 2017).

Currently, in the global economy, data has become the key and most vital asset. In 2027, the global data sphere will reach an estimated size of 291 zettabytes, up from a forecast of 120 zettabytes in 2023. Cross-border data flows are crucial to digital trade, the development of artificial intelligence, financial services, and national security intelligence, and are estimated to have an economic contribution of almost USD 3.4 trillion in 2023. (Seong et.al, 2022) With the centralization of data-processing capabilities in the hands of a few digital giants, primarily the United States, the European Union and China, data governance has shifted from a technical/administrative concern to a first-order geopolitical concern. In this context, important state actors have adopted very different approaches towards data sovereignty, which, in turn, is leading to greater fragmentation of the global digital order.

US calls for open data movements and selectively

enforces extra-territorial restrictions on foreign technology actors. That the European Union has a rights-based regulatory framework, and that it has an extra-territorial dimension, is an example of what Bradford calls the 'Brussels Effect' (Bradford, 2020). China has declared its full cyber sovereignty, and has built the most advanced digital governance system in the world. Russia has been working towards becoming tech independent by setting up a national internet. India is at an early stage of a hybrid state between these extremes. This interaction of the frameworks is creating what experts are terming the splinternet, the division of the internet, which is once again united, into national and regional digital ecosystems (Mueller, 2017). This work provides a theoretically sound, and experimentally tested analysis of this change.

1.1 Problem Statement

Although there is growing interest in data sovereignty both in the scholarly and policy community, there is a significant theoretical and empirical gap. Much of the literature focuses on a particular national model or single regulatory instrument and the systemic geopolitics that results from the interaction of conflicting models at the global level is under explored. The quantitative aspects of digital fragmentation, measured regulatory difference that divides data flows, limits technology interoperability and refashions digital trade, remain under-documented. Moreover, the governance implications of determining the Global South's digital fate in Washington, Brussels and Beijing are barely discussed in the literature. Finally, this study fills these gaps with a theoretically integrated, empirically grounded and comparably structured analysis based on data current until 2026.

1.2 Research Hypothesis

	Hypothesis Statement	Direction	Status
H1	The more countries assert their data sovereignty, the more that global internet infrastructure and cross-border data is actually becoming fragmented.	Positive	Testable
H2	Compliance costs grow for multinationals digital businesses when there is regulatory difference between the US, EU, and China.	Positive	Testable
H3	Countries with strong digital infrastructures and big domestic markets have more geopolitical muscle to influence global data governance regulations.	Positive	Testable

H4	Lack of an institutional multilateral digital governance framework is having a significant impact on intensifying competitive dynamics and driving digital fragmentation.	Positive	Testable
H5	Economic openness factors are never more important determinants of a state's data localization policy than are national security considerations, regardless of the type of regime.	Directional	Testable

1.3 Research Question

No.	Research Question	Type
RQ1	What is the impact of the strategic assertion of national data sovereignty of major nations on the architecture of the global digital order since 2013?	Primary
RQ2	In which ways the data governance frameworks of the US, EU and China reflect distinct geopolitical strategies and political economies?	Comparative
RQ3	How much do regulatory fragmentation in global digital markets cost, in economic and political terms?	Empirical
RQ4	Explicative power of the concept of weaponised interdependence for the issue of data governance of big digital powers?	Theoretical
RQ5	What institutional changes are needed internationally in order to balance the different national frameworks in a functionable global governance system?	Policy

1.4 Objectives

The study has the following objectives

1. To theorize data sovereignty as a geopolitical tool in the interconnected world of digital geopolitics and weaponized interdependence.
2. To analyze data governance models of five major powers from various perspectives of analytical dimensions to compare them
3. To document statistical and empirical dimensions of fragmentation in digital domain
4. To construct a conceptual model, which would causal relationships among sovereignty assertion, fragmentation, and regulatory competition at global level
5. To build up a composite Digital Sovereignty Fragmentation Index
6. To devise practical policy recommendations for multilateral governance reforms

1.5 Significance and Scope of the Research

It covers the period from 2013 to 2026, and follows the main wave of digital sovereignty laws post-Snowden revelations, GDPR, China's Cybersecurity Law, Russia's Sovereign Internet Law, India's Digital Personal Data Protection Act and the ongoing proliferation of data localization requirements in over 100 countries.

Geographically, the study includes the five major regulatory blocks. Thematically, the research covers data localization policy, cross-border data flow governance, cybersecurity doctrine, digital infrastructure competition, platform regulation, and international digital trade law. The study will be of interest to academics of international relations, political economy, and internet governance, as well as to policymakers grappling with the nexus of sovereignty, technology, and global order.

2. Literature Review

2.1 Digital Configuration of classical Sovereignty

From its philosophical expression to this day, the concept of sovereignty has been put in question. Jean Bodin's concept of sovereignty was that of absolute and perpetual power. States, the ultimate guarantors of order, were established by Hobbes Leviathan. It was these ideas that were institutionalized in the "Westphalian" settlement, and which became the "building blocks" of the architecture of territorial sovereignty, which has governed the behavior of international relations for almost 400 years (Mayer et al., 2025). The most analytically rigorous paradigm developed to explore digital challenges to sovereignty is the one developed by Stephen Krasner and which makes a

distinction between four types of sovereignty: domestic, interdependence, Westphalia and international legal sovereignty. Keohane and Nye's complex interdependence and overlapping governance systems envisioned possibilities for the diffusion of the authority of the state across levels. However, with the advent of the digital age, there is a paradox as data flows are global, whereas states are increasingly asserting control over them via digital means, data localisation laws, platform regulation, cyber security legislation and infrastructure nationalism. (Falencik, 2021) Sovereignty does not seem to be fading, but rather morphing, into hybrid forms of territorial sovereignty and administration of digital sovereignty.

2.2 Conceptual evolution of digital sovereignty

When referring to digital sovereignty, it is common to refer to a state's capacity to control its digital infrastructure, its data assets and digital activities within its borders. The idea has gone through three generations: the first was a rather narrow one focusing on technical internet governance, the second was a response to the Snowden revelations on national data localization and cybersecurity laws, and the third generation includes full-fledged industrial policy, AI governance, platform regulation and export of regulatory norms abroad. The European Commission's concept of digital sovereignty is the EU's capacity to be open and connected yet sovereign and autonomous within the digital sphere: the very essence of the dilemmas of digital governance today (Glasze et al., 2023).

2.3 Digital Geopolitics and the nexus of data, space and power

The classical geopolitical theories associated the political power to control territory and strategic resources to sea power doctrine of Mahan and Heartland thesis of Mackinder. These dynamics are being moved into the digital space, the new geopolitical cyberscape, where control of digital infrastructures, platform ecosystems and data are generating a new structural power. Bai views this as a data-space-power nexus, where data is a strategic resource, digital space is an infrastructural environment of competitiveness and regulatory power is the key instrument of geopolitical power (Bai 2026). The idea of weaponized

interdependence proposed by Farrell and Newman implies that the governments of countries at the heart of the global economic network can use technology to create a chokepoint effect or a panopticon effect for oppressive purposes (Farrell and Newman, 2019). The Brussels Effect in Bradford demonstrates how with the power of regulation, sovereignty can be extended beyond the nation-state through the application of market leverage, not military or economic force (Bradford, 2020).

2.4 Splinternet and Fragmentation

The discussion on the 'internet of the things' has moved from theory to fact. Mueller suggested a dynamical of fragmentation at systemic level which stemmed from struggles around sovereignty. The economic costs of information nationalism were explained by Chander and Le. The OECD states that the amount of restrictions on digital trade has doubled since 2017. There have been almost three times as many internet restrictions and shutdowns since 2019, according to Freedom House. But that's not the only thing that has changed, splinternet is no longer metaphor, it has become a quantifiable trend in the web (Mueller, 2017). Three lines of research have been underdeveloped: competing national frameworks are under theorized, quantitative aspects of fragmentation are poorly documented and dilemmas of governance of the Global South remain under analyzed.

3. Theoretical Framework and Conceptual Model

The study is based on a synthetic theoretical framework integrating three different complementary analytical lenses: (i) the data-space-power nexus as a map of three-dimensional geopolitical competition over data resources, digital infrastructure and regulatory power; (Bai 2026) (ii) weaponized interdependence (Farrell and Newman, 2019), a theory of how structural centrality in global digital networks can be coercively leveraged; and (iii) the Brussels Effect as a theory of the extraterritorial projection of regulatory norms through market power Effect' (Bradford, 2020). These are put together and lead to a complete analytical apparatus at bilateral, regional and systemic level of analysis.

3.1 Conceptual Model

State Actors	Mechanisms of transmission	Moderating Variables	Outcomes
Global South, India China (PRC), Russia United States	Technology Decoupling, Data Localization Mandates, Norm Contestation, Regulatory Divergence, Infrastructure Competition	Capacity and Operations of Multilateral Institutions Market Size and Tech Capability Domestic Political Economy Type Depth of Economic Interdependence Institutional Capacity Alliance and Partnership Structures	a) Digital Fragmentation (Splinternet) b) Regulatory Hegemony (Brussels Effect / Beijing Effect) c) Managed Interdependence (Bilateral Frameworks): Both parties are sustained and grow without significant change in the relationship.

This model leads to five testable propositions: (P1) data as strategic resource gives rise to competition for regulatory primacy; (P2) infrastructure centrality brings about structural power; (P3) competing governance paradigms create emergent fragmentation without a multilateral rules framework; (P4) economic interdependence dampens but does not remove pressures of fragmentation; (P5) bilateral accommodation may be a substitute but not a replacement for multilateral governance solutions.

4. Research Methodology

This study is a secondary data study and has a qualitative and comparative research design, and a most-different-systems design. Of the 5 cases, the US, EU, China, India, and Russia, the variation in factors other than the causal condition (digital globalization/ strategic value of data) and the focal factor (political system, economic model, strategic culture) is maximal. This provides the maximum possible leverage for analysis: the closer are the patterns of sovereignty assertion, the more distinct are the systems, the more the causal explanations should focus on the common structural conditions and less on idiosyncratic factors.

Component	Design Choice	Justification	Sources
Paradigm	Critical Realist and Interpretivist	Qualitative analysis is needed in the case of complex causal mechanisms.	Academic literature (2020-2026)
Primary Method	Descriptive Statistical Analysis	Most-different-systems design	Policy documents, legal texts, or other documents that have implications for policy.
Secondary Method	Longitudinal: 2013-2026	Quantify fragmentation dimensions	ITU, UNCTAD, WB, OECD, McKinsey
Temporal Scope	Legislative texts and trade data, security indices and market statistics	Legislation to be implemented to restore the wave of sovereignty.	The government reports, think tanks
Data Types	Plus DSFI construction (Cross case comparison)	Triangulation for validity	Freedom House, Gartner, IDC, ECIPE,

Analytical Strategy	Triangulation of sources from a variety of independent datasets (30+)	Qualitative and quantitative synthesis of the data	Academic journals (2020-2026)
Validation	Comparative Case Analysis (5cases)	Reduces single-source bias	Multiple authoritative sources

5. The Statistical landscape of Data Sovereignty: Empirical Analysis

5.1 International Data Economy (2022-2026)

Indicator	Finding	Year	Source
All data created, captured, copied and consumed globally	120 zettabytes	2023	IDC / Statista 2024
Projected global datasphere	291 zettabytes	2027	IDC Digital Universe
Economic contribution of cross-border data flows.	USD 3.4 trillion	2023	McKinsey GI 2024
Global digital economy (as a share of world GDP)	~15.5%	2023	UNCTAD 2024
The value of the public cloud services market around the world	USD 679 billion	2024	Gartner 2024
It is estimated that the value of the cloud will be \$180 billion by 2020.	USD 1.2 trillion	2028	IDC Cloud Market Report
Globally, there are laws that mandate data localization, in the national context.	144 laws / 62 countries	2023	ITIF / WEF 2024
Total GDPR fines, across all the EU member states	EUR 4.5 billion	2018-2024	GDPR Enforcement Tracker
Cloud market share, AWS, Azure or Google, in the USA	~65% of global cloud	2024	Synergy Research Group
Capacity in data centres, China, as percentage of world	~23%	2023	IEA 2024
Every year, millions of dollars are spent on the costs of data localization in the global digital trade.	USD 104 billion/year	2023	ECIPE 2023
Top 3 Global Cyber Security market value	USD 202 billion	2024	Cybersecurity Ventures 2024
Two or multi-sided data agreements with bilateral or regional focus.	130+ agreements	2024	OECD Going Digital 2024
The value of the global AI market	USD 196 billion	2024	Statista AI Report 2024
Submarine cables around the world	600+ cable systems	2024	TeleGeography 2024

Percent of internet traffic that passes through the United States.	~38%	2023	Cloudflare Annual Report 2024
An enterprise data breach costs, on average globally:	USD 4.88 million	2024	The insights are based on the IBM Cost of Breach 2024 research.
AI Strategy countries	58 countries	2025	OECD AI Policy Observatory

5.2 Comparative National Data Governance Profiles (2024-2025)

Dimensions	United States	China	European Union	India	Russia
Primary governance model	Market-driven / Liberal	Security-Sovereign	Rights-based / Regulatory	Hybrid Developmental	Self-reliant / Isolationist
Data localization requirements	Minimal: Sector specific (HIPAA, ITAR etc)	Extensive (DSL 2021, CSL 2017, PIPL 2021)	Conditional adequacy (GDPR Ch. V)	Significant (DPDPA 2023)	Extensive – Laws 242-FZ and 90-FZ
Internet Freedom Score 2024	72/100 Free	9/100 Not Free	65-80 Mostly Free	50/100 Partly Free	21/100 Not Free
Data laws in the major countries 2010-2025	12 (sectoral)	9 (comprehensive)	9 (comprehensive)	5 (evolving)	7 (evolving)
As a share of the world's tech market capitalization	~58%	~23%	~8%	~4%	~1%
The degree of cross-border data flow index (0-100)	82	13	57	41	17
The highest power of the fine regulator	Not a single FTC, instead a collection of fragments that are also state AGs.	Up to CNY 50M + criminal liability	Up to 4% of annual turnover in the world.	Up to INR 250 Cr (~USD 30M)	Up to 18M RUB (~USD 200K)
AI compute capacity (global share %), by percentage	~40%	~33%	~10%	~4-5%	~2%
Regime of platform content moderation.	Section 230 (broad immunity)	CAC platform licensing system	DSA/DMA gatekeeper regulation	IT Rules 2021	Sovereign Runet isolation
ITU stance on expansion of its internet governance role	Against (multistake holder model)	Strongly for	Cautious (normative approach)	Moderate	Strongly for

5.3 Cost and Consequence of Digital Fragmentation

Cost Dimension	Estimated Impact	Affected Actors	Time Horizon	Source
Divergent GDPR / DSL / DPDPA Compliance for MNC.	USD 20-40B a year NEW compliance	Global MNCs that operate in the EU, China, India segment.	Annual ongoing	IAPP/Deloitte 2024
Trade diversion effects of data localization requirements	Loss of USD 104 billion a year in digital trade.	Exporters and importers of digital files all	Annual compounding	ECIPE 2023

		over the world.			
The loss in efficiency of the cloud ecosystem.	Up to 25% loss in global cloud allocation efficiency	Cloud providers and enterprise users	Medium-term	IDC 2024	
Reduced AI R&D from data siloing	Loss of 3-5% of the global output of AI innovations per year	Technology sector globally	Long-term 2025-2035	OECD AI Outlook 2024	
Loss of cyber security due to internet isolation at national level.	35% bigger attack surface and ~40% longer breach detection.	Governments, critical infrastructure	Ongoing	IBM X-Force 2024	
The situation in developing countries regarding digital exclusion.	US\$ 500 billion opportunity loss of the digital economy	Africa, Asia, LatAm (Global South)	2025-2030	World Bank Digital 2024	
Uncertainties in the legal environment for cross-border digital trade.	The number of cross-border digital litigations has increased by ~30%.	Compliance / legal industry; digital SMEs	Medium-term	WTO monitor 2024	
Dubbing of submarine cables and Securitisation.	A USD 10-20 billion extra annual cost to infrastructure.	Governments, ISPs, hyperscalers	Medium-term	TeleGeography/JRC 2026	
Compliance of financial services data sovereignty.	The annual cost increase for banks around the world is USD 8-12 billion.	Financial services, financial technology, payment services.	Annual	FSB Digital Finance 2024	
Fragmentation in semiconductors supply chain	USD 50-100 billion extra investment to duplicate	Semiconductor industry, governments	2024-2030	BCG 2024	

6. Comparative Analysis: 5 Models of Data Sovereignty

6.1 The United State

In the past, the United States has been a strong proponent of free cross-border data flow for economic and geopolitical purposes: the economic and business models of technology companies based in the United States, which represent approximately 58 percent of global technology market capitalization, depend upon free cross-border data flow. The US has included data liberalization clauses in the US-Mexico-Canada Agreement (2020) and US-Japan Digital Trade Agreement (2019), and has been pushing back against data localization clauses at WTO and bilateral trade negotiations. Unlike other countries, there is no federal omnibus privacy law in the U.S.

as of 2025 and the framework is typically sectoral, meaning that different regimes govern health data, financial data, children's data and export-controlled technical data.

But, US data governance is a strategic contradiction: pro-global data liberalization and heavy-handed extraterritorial data restrictions against foreign tech actors that are considered security threats. Starting in May, the CLOUD Act 2018 requires the handover of data of US cloud service providers to domestic law enforcement requests regardless of where the data is stored, and this has been at odds with data protection regimes in Europe. These are all part of a framework of data de-coupling specifically against China and other countries of concern: The Foreign Investment Risk Review Modernization Act, Export Control Reform

Act 2018 and 2024 Executive Order on Preventing Access to US Sensitive Personal Data. The ban on Huawei, the forced sale of TikTok, and the CHIPS and Science Act 2022 are all parts of a large-scale industrial policy stance in which data governance is a tool to engage in strategic competition.

The Sino-American technology competition has played a major accelerating role in this selective decoupling trend. The most significant restructuring of U.S. data and technology governance since the Cold War is the export controls for advanced semiconductors, U.S. cloud services for the training of AI models on Chinese companies, and the Entity List designations of Chinese AI companies. By contrast, the US-EU relationship is managed by institutional accommodation, with the EU-US Data Privacy Framework allowing for transfers of data between the EU and the US, provided that certain conditions are met, but with doubts about the legal longevity of the framework in light of ongoing conflicts between US surveillance law and EU privacy rights (Bai, 2026).

6.2 China

The concept of cyber sovereignty is the basis of China's data governance, which means each State has complete sovereignty and regulation authority over its own part of the Internet, free from the interference of other States. The doctrine is an obvious challenge to the liberal internet governance model, and has been promoted in the agendas of WSIS, IGF and ITU since the mid-2000s and has been picked up by many states in the Global South that have been enticed by China's technology deals. Chinese cyber sovereignty architecture includes four pillars: enacting comprehensive laws, constructing the technical infrastructure (the Great Firewall and the Golden Shield Project), managing platforms by CAC licensing and promoting international norm through Digital Silk Road investment (Mayer et al., 2025).

The data under China's laws, such as the Cybersecurity Law, Data Security Law, Personal Information Protection Law and Cross-Border Data Transfer Security Assessment Measures are divided into different categories according to their importance, and the transfer of important data or large personal information is subject to security inspection. China has also established the National Data Administration (NDA) which focuses the

powers of data governance (Yilmaz, 2026), indicating its desire to consider data as a strategic asset to be governed at the national level, rather than a commercial product. The Digital Silk Road is the most influential side of China's digital geopolitics overseas, as part of the BRI. By supplying 5G infrastructures to over 100 countries and with the help of Alibaba, Tencent cloud services, Union Pay payment and surveillance technology packages, China is certainly creating a set of technological dependencies that are structurally bending the recipient countries towards Chinese regulatory norms (Rahman, 2025).

6.3 European Union

The European Union is the most ambitious attempt worldwide to establish digital sovereignty by means of rights law, and by extra-territorialization of normativity. The GDPR gives a lot of rights in relation to personal information, to any company that processes information of EU citizens regardless of where they are incorporated and gives very strong sanctions for non-compliance. As a matter of fact, up to 2024, the total amount of penalties and fines imposed as a result of the cumulative GDPR enforcement actions is already in excess of EUR 4.5 billion, and the majority of these sanctions are imposed on Meta, which now exceed EUR 1.3 billion.

The Digital Markets Act 2022 and the Digital Services Act 2022 broaden the definition of who is covered by the EU regulation to include platform companies as gatekeepers, which are thus subject to asymmetric obligations in platform competition policy and content governance. The Brussels Effect has its impact on AI governance, too, as the European AI Act 2024 is the world's first comprehensive binding AI regulation, which introduces requirements based on risk for AI systems deployed in the EU market, regardless of where they are developed. The institutional structure of a European data space is set up by the Data Governance Act 2022 and Data Act 2023 which will enable Europe's industrial assets to become competitive digital resources.

The EU is facing strategic dilemmas which are expressed in the JRC policy brief such as how to export values while forming alliances internationally, how to reduce dependence on infrastructure without being disconnected from the rest of the world, how to use economic instruments

and remain open to the market, and how to reconcile social cohesion and respect for individual freedom. Modular resilience, reduction of critical dependencies in a targeted way and strategic openness, without being US market dominant or Chinese comprehensive sovereign are all hallmarks of the EU's digital sovereignty strategy (Glasze et al., 2023). The Safe Harbor, Privacy Shield, and DPF cycle across the Atlantic is illustrative of the current suite of institutional mechanisms that embodies a set of structural tensions between EU views on privacy and US views on surveillance.

6.4 India

This data governance journey in India presents a confluence of tensions for the large democratic developmental state that desires to be both welcoming to foreign investments in the digital economy and mindful of the rights of citizens to their data, assert control over critical data infrastructure and leverage its huge repository of data for economic development (Jansen et al., 2023). DPPDP Act after 10 years of legislation introduces a consent-based framework for processing of personal data and has granted certain significant exemptions to state authorities and for national security. Transfer of data to government-notified trustworthy territories across borders is another and more flexible architecture than the GDPR's adequacy system and China's security-assessment system, and is more consistent with sovereignty (Tan, J. 2026).

The unique combination of state-led digital infrastructure and market-led innovation in institutional innovations such as the Data Empowerment and Protection Architecture, India Stack provides a distinctive blend of innovation and digital empowerment. UPI has handily transacted over 13 billion transactions every month in 2024 as a testament to the potential of public digital infrastructure. India's approach is hence different from the other four cases which are enhanced

developmental benefits via state-led infrastructure, and the gradual extension of regulatory powers.

6.5 Russia

The most extreme form of the security-sovereign model is the Russian data governance model, specifically designed to address the weaknesses of data infrastructure in Russia to intelligence collection by the West and only allow the movement of politically controlled data. Personal data localization legislation requires that personal data of Russian citizens be stored on Russian servers, and if services do not comply with this requirement, they are blocked, for example, LinkedIn, 2016. According to the Sovereign Internet Law, Federal Law 90-FZ, which is in force in 2019, but part of the law was partially activated during the Ukraine conflict of 2022, deep packet inspection (DPI) equipment must be installed at the major internet exchanges points to make it possible to filter traffic and isolate the national network.

The fact that Russia has the capacity to block digital platforms systematically since the beginning of the invasion in February 2022, its blocking of Facebook, Instagram and several Western news outlets, demonstrates that Russia has the DPI capabilities and the massive economic impact of digital isolation in Russia: In the sectors affected, the volume of e-commerce on the blocked platforms was estimated to have dropped by 30-40 percent, while the number of downloads of Russian VPNs increased by approximately 2,000 percent in March 2022 alone. The domestic alternatives' development is part of Russia's long-term plans to build alternative digital infrastructure that can be used without the support of western systems, such as social network VK, government services Gosuslugi, payments system Mir or financial messaging service SPFS, the experts say.

7. Competition, Alignment and Systemic Fragmentation: Geopolitical Dynamics

7.1 The bilateral axis of digital Geopolitical competition

Bilateral Axis	Primary tension	Institutional Mechanism	Fragmentation Risk	Current status
US-China	Decoupling of technology, AI vs semiconductors, Data access, Platform markets	Export controls (BIS), CFIUS, Entity List, Executive Orders with data	Very High	Escalating/Partial decoupling in progress
US-EU	Surveillance law and	EU-US DPF (2023) /	Moderate	Set up and managed

	privacy; CLOUD Act, regulation of platform, divergence of AI governance	Trade and Technology Council (TTC).		as an institution; not structure resolved.
EU-China	Market access, regulatory norms, infrastructure dependency, SC de-risking	Two-way dialogues with the EU, Sectoral MOUs	Moderate-High	Contested (2023-2026) - EU de-risking strategy in place.
US-Russia	Cyber-attacks, information operations, sanctions, technology denial	No formal mechanisms for cyber governance, NATO cyber coordination.	High	Hostile, Deep Decoupling, Dual Digital Systems
India-Major powers	Data sovereignty, strategic autonomy	DPDPA regulations, Quad tech pacts.	Moderate	Strategic, evolving, active
Global South-Major powers	Digital colonialism, extractivism of data, dependence on technology, exclusion in governance	G77 digital proposals / AU Data Framework	High	Structurally disadvantaged, voice multilaterally grows

7.2 Case evidence: Weaponized Interdependence in practice

The multiple concrete cases of the interplay of contemporary digital geopolitics powerfully validate the weaponized interdependence theory of Farrell and Newman (2019). The 'chokepoint' logic of denying network access has been seen in: (i) US semiconductor export controls, BIS October 2022 rules & 2023-2024 expansions, to deny China's AI firms access to advanced NVIDIA H100 chips, and to limit China's frontier AI; (ii) exclusion of Huawei from allied 5G networks – to limit embedding intelligence-gathering capacity in critical telecom infrastructure; (iii) SWIFT exclusion of Russian banks (2022), leveraging US-EU centrality in global financial messaging for geopolitical coercion. The panopticon mechanism is demonstrated by, for example, the so-called PRISM programmed of the National Security Agency

(NSA), exposed in 2013, which placed mass surveillance of foreign communication traffic at the center of the US internet by leveraging the key role of the USA in the global internet routing system.

The China's response is much more comprehensive: the CIPS cross-border interbank payment system, currently used by 1,400+ financial institutions in 110+ countries, is an alternative to SWIFT; Digital Currency Electronic Payment (e-CNY) is a sovereign digital currency; HMN Technologies is an alternative submarine cable constructor; and the dual circulation industrial strategy and big fund semiconductor program are domestic capability responses to export controls. These measures are a systematic strategic counter to weaponised interdependence aimed at minimizing the exposure of network centrality while creating other network structures that create leverage over others.

7.3 The Splinternet: Quantifying fragmentation

Fragmentation Indicator	2017	2020	2023	2025	Trend	Source
National laws on localization of data (count)	17	62	144	160+	Sharply increasing	ITIF / WEF 2024
Countries blocking and/or restricting major global platforms	26	48	72	80+	Increasing	Freedom House 2024
Internet shutdowns by the government, which are ordered once a year.	75	155	187	200+	Increasing	NETBLOCKS / Access Now 2024
Digital trade restriction index (2017=100) (OECD)	100	148	187	200+	Accelerating	OECD Digital Trade 2024
Data adequacy agreements on a bilateral / regional level	12	45	130+	150+	Rapid bilateral substitution	OECD Going Digital 2024
National AI / data governance policies and strategies	8	50	85	120+	Expanding globally	OECD AI Observatory 2025
National digital ID that do not interoperate with each other.	15	42	78	95+	Increasing	World Bank ID4D 2024
List of countries that have cyber security laws.	35	58	95	110+	Converging (divergent substance)	ITU GCI 2024
The number of monthly active users (in millions) using VPN services in the world. (Approximately)	240M	480M	840M	More than 1 billion	Reflects restriction escalation	Global Web Index 2024
Restriction measures in the field of the cross-border data flow (WTO)	40+	95+	160+	190+	Accelerating	WTO e-commerce monitor 2024

7.4 The challenges of multilateral Digital Governance: The institutional gap.

The lack of an overarching and binding multilateral framework for digital governance is the most important conditions for the fragmentation described above (Yusuf et al., 2016). The WTO Joint Statement Initiative (JSI) on e-commerce, which was started in 2019 by 90 members, has been floundering in its efforts to come up with rules on data flows, data localization and source code protection, with India and South Africa not

participating on the grounds of development. Western democracies have been wary of intergovernmental replacement of the multistakeholder model in the process of internet governance to which the ITU has wanted to expand. Internet Governance Forum (IGF) continues to be a non-binding and non-enforceable forum. The consequence is a governance gap at the systemic level that has been filled, at least partially, but not adequately, through bilateral, regional governance (UNCTAD, 2024).

Framework Or Institution	Scope	Binding Authority	Key Limitation	Coverage Gap
JSI on e-commerce by WTO	Rules on digital trade such as data flows.	Partial if concluded	Divergence of US, China and India, India / SA not participating	Developing country buy-in
Trusted Govt. is a declaration of the OECD. Access to Data (2022)	Principles to access government data	Non-binding soft law	Excludes China and Russia or any other countries not in the OECD.	China, Russia, most Majority (Global South)
The G20 Osaka Track is Data Free Flow with Trust (2019)	DFFT political commitment	Non-binding	Lack of implementation processes; no progress made.	Enforcement capacity
The UN Internet Governance Forum (IGF) is an international multi-stakeholder forum.	Multi-stakeholder dialogue	None	No mandate – Consultative only.	Legal force; implementation
ITU	Technical standards/internet governance	Limited (standards only)	Controversial inroads into policy for governance	Governance legitimacy
Cross-Border Privacy Rules (CBPR) under the APEC.	Data transfer certification in Asia-Pacific region.	Voluntary certification	Limited (non-EU) membership.	The code for the EU and India is incompatible with the code from China.
CERTIFICATE EU-US Data Privacy Framework (2023)	Transfers of personal data across the Atlantic Ocean and the European Union and EFTA/EEA areas.	Bilateral & challenge risk to the judge's ruling	There may be some issues with Schrems III challenge.	Non-transatlantic actors
RCEP Digital Chapter	Asia-Pacific e-commerce rules	Binding for 15 members	Poor data arrangements; substantial carve-outs	Outside the RCEP - US, EU, India
AU Data Policy Framework 2022	African data governance guidelines are also in the process of being developed.	Non-binding	Implementation capacity constraints	Enforcement; technical infrastructure

8. Results and Discussion

8.1 Hypothesis Testing Results

Verdict	Key Evidence	Confidence	Qualification
H1 Supported	National data localization laws increased 847% (17 to 144+) from 2017-2023; internet shutdowns increased 167% (75 to 200+); OECD digital trade restriction index up 100% (2017-2024).	High	Fragmentation quantifiable and speeding up

H2	Supported	Additional costs of complying with law for MNCs, USD 20-40 billion/year (IAPP/Deloitte); GDPR fines of EUR 4.5 billion; compounding costs for firms in EU, China, and India due to conflicting DSL/PIPL/DPDPA/GDPR requirements.	High	Quantitatively documented
H3	Partially Supported	The Chokepoint leverage is the semiconductors export controls, created by the dominant position of the US cloud (65%) and AI Compute (40%). There is empirical evidence of Brussels Effect registered. But, in China's Digital Silk Road, norm projection is provided by infrastructure investments.	Medium	There are more than one pathway to norm influence.
H4	Supported	As of 2025, no binding global data flow framework exists, and the WTO JSI has stalled from 2022–2025, while IGF is non-binding, the result of a lack of institutional action at the multilateral level.	High	Finding with the best available evidence of direct observation
H5	Partially Supported	Thus, China DSL/CSL, Russia 242-FZ and 90-FZ as well as India DPDPA security exemptions on the one hand prove security first, while the US-EU DPF on the other hand shows that economic dependence can also be more important, and for liberal democracies, the final security is not absolute.	Medium	How regimes affect outcomes (mediation)

8.2 Digital Sovereignty Fragmentation Index (DSFI)

This study creates a new composite Digital Sovereignty Fragmentation Index (DSFI) that is based on six dimensions of each major actor, which are weighted as follows: data localization extent (0-10), platform access restrictions (0-10), cross-border data flow friction (0-10), regulatory

divergence from international baseline (0-10), infrastructure decoupling (0-10), and multilateral cooperation deficit (0-10, reversed, higher = less cooperative). The scores are combined together and given a score on a 0-100 scale. This index is intended as a guide for analysis based on the best information available and should be used as a directional indicator and not a precise measure of anything until it can be empirically validate.

Actor	Data localization	Platform Restriction	Data Flow friction	Regulatory Divergence	Infrastructure Decoupling	Multilateral Cooperation Deficit	DSFI
US	2	1	2	5	7	5	32 Low
EU	4	2	4	7	4	4	42 Moderate
China	9	10	9	9	9	9	90 Very High
India	5	4	5	5	4	5	47 Moderate-High
Russia	9	9	9	9	8	9	85 High
Global Average	5.8	5.2	5.8	7.0	6.4	6.4	59 High

The DSFI scores show that there is a wide gap between the international digital governance landscapes. On the high fragmentation side, China and Russia have fragmentation values of 85–90 (DSFI); selective decoupling is practiced in the US where the fragmentation scores is relatively low (DSFI 32). EU and India are in intermediate positions which indicate hybrid governance positions. The global average DSFI of 59/100 suggests that fragmentation is no longer a concern on the fringe but is part and parcel of global digital governance architecture, with significant consequences for the future of the global digital economy (Yusuf et al., 2016).

8.3 Discussion: to identify shortfalls and opportunities for Data Sovereignty as Systemic Transformation.

Three conclusions in analysis surface. First, assertion of data sovereignty is a structural change on the international system. The expansion of data localization laws, the split of the semiconductor industry and cloud services, the establishment of digital payment systems (SWIFT and CIPS) and parallel digital payment systems (Visa/Mastercard and Mir/UnionPay), and the different AI governance systems are just a few of the trends that indicate a qualitative change in the architecture of global digital interdependence, which will continue

regardless of what happens politically in the short term (Tan,J. 2026).

Second, there is a systematic variation of the form of asserting sovereignty according to the type of political economy (Mayer et al.,2025). Liberal market economies utilize targeted regulation on strategic sectors, and remain open to markets. Rights-based regulatory states have a normative power with the leverage of the market. For security-sovereign states, data governance is a means of state control in general. Hybrid developmental states pragmatically move between the regimes. These systematic variations corroborate the idea that a data governance strategy is a reflection of a configuration of the political economy, and not just a random political decision (Papyshev, 2026).

Thirdly, the institutional design for the governance of digital fragmentation is seriously insufficient and declining (Li, 2026). The result of non-binding forums (IGF), on-going negotiations (WTO JSI) and geopolitically limited institutions (ITU) is that key regulatory conflicts are left to bilateral channels which are neither transparent, nor systemically stable. The second-best institutional solution is the growing number of bilateral data adequacy agreements, as of 2024, more than 130 bilateral agreements are in place.

9. Policy Implication and Recommendation

Level	Recommendation	Rationale	Priority	Lead Actors
Multilateral	Conduct WTO negotiations to negotiate binding data flow rules, mutual recognition of data adequacy and flexibilities for Global South parties in the WTO Digital Goods and Services Agreement.	Forging normative convergence, which doesn't need US-China agreement; stepping stone towards binding rules	Urgent	UN Secretariat
Multilateral	Set up a UN Intergovernmental Panel on Digital Governance (IPDG) with an analytical and norm-recommendation mandate, with multistake holder participation, similar to IPCC.	As the Global South is at risk of falling into digital exclusion, regional frameworks create constituencies for multilateral reform.	High	The ASEAN, AU, and World Bank are also involved in the project.
Multilateral	Accept a Global Framework on Cross-Border Data Flows in the UN Global Digital Compact – non-binding principles and, voluntary, implementation pathway.	Recurring invalidation cycle = systemic uncertainty, legislation fixing = no judicial arbitration risk.	High	Growth and development of the U.S. agriculture sector and the

				EU Commission.
Regional	Enlarge the scope of the ASEAN Digital Framework; African Union Data Policy Framework and CARICOM digital governance initiatives and include capacity building through funding from advanced economies.	Undifferentiated localization does not have proportionate security benefits and costs disproportionately.	High	National legislators
Bilateral	Legislatively make EU-US DPF domestic law to protect against Schrems III invalidation; modify CLOUD Act to eliminate extraterritoriality issues with EU data protection law.	Strategic de-risking, but not autarky; open but not powerless digital EU	Urgent	European Commission
National	Adopt graduated proportionality test for data localization; impose localization requirements only if it is shown that data security needs require it, and a cost-benefit analysis is conducted.	Technical standardisation contributes to compliance savings, functional integration under political fragmentation	Hight	Standards bodies, industry
National	Foster JRC 2026 modular resilience approach that involves a calibrated depenultimisation of critical infrastructures (cloud, AI, semiconductors), while keeping open.	Forging normative convergence, which doesn't need US-China agreement; stepping stone towards binding rules	High	UN Secretariat
Industry or Technical	Create Global Data Interoperability Standards Consortium under IETF/ISO/W3C to create technical standards to allow cross-regime data exchange without the need for legal harmonization	As the Global South is at risk of falling into digital exclusion, regional frameworks create constituencies for multilateral reform.	Medium	The ASEAN, AU, and World Bank are also involved in the project.

10. Limitation of the Study

This study has a number of methodological and empirical limitations. First, the use of secondary data limits the conclusions that can be drawn as it is only as good as available statistics and documentation of policy; there is a large degree of uncertainty around measurement of the enforcement practice, the actual cost of compliance and the implementation of bilateral agreements. Second, despite being conceptually sound and relying on authoritative indicator data, the Digital Sovereignty Fragmentation Index (DSFI) has not yet been statistically validated using primary survey data, and it should therefore be used as an analytical tool to inform practical activities and decisions. Third, five cases studies have been chosen which do

not include significant regulatory actors, namely Brazil, Japan, South Korea, Singapore and the emerging ASEAN Digital Framework. Fourth, digital geopolitics are dynamic and findings regarding particular agreements and legislative provisions might need to be revised. Future studies must gather primary quantitative data on the costs of fragmentation via enterprise survey techniques, expand comparative analysis to cover the Global South and put the DSFI to the test with empirical outcomes data (Li, 2026).

11. Conclusion

In this paper we have contended that the geopolitics of data sovereignty is one of the key structural changes of the current international regime. Amidst current debates and developments, the Westphalian

notion of sovereignty, based on territorial authority, fixed borders and the absence of foreign influence, is being reframed in a digital sense into a hybrid version that is shaped by data localization, regulation systems, cyber-security and the management of critical digital infrastructure. The reconfiguration reflects and intensifies the current asymmetries in terms of technological capabilities, market power and institutional capacities in the international system.

The analysis of five major actors of data governance shows that there is a uniform structure: the data governance model of each of the actors is not simply a domestic regulatory option, but a geopolitical strategy based on the actors' structural position in the global digital economy, political economy configurations, strategic cultures, and geopolitical threat perceptions. Many countries strive for a hybrid approach to developmental sovereignty, like India, while others seek a comprehensive cyber sovereignty, like China, which is exporting its cyber governance model via Digital Silk Road infrastructure or selective decoupling, like the U.S., or regulatory extraterritoriality and the Brussels Effect, like the EU, or self-reliance at the expense of connectivity, like Russia.

The Digital Sovereignty Fragmentation Index, created as an original analytical contribution, shows that digital fragmentation is structurally embedded, as the average score is 59 out of 100 for all the

countries. The economic losses are significant and growing, for example, more than USD 104 billion per year in digital trade diversion, USD 20-40 billion MNC compliance spending and up to USD 500 billion in foregone Global South digital economy by 2030. But so are the security and democratic consequences such as the degradation of cybersecurity, the export of surveillance infrastructure, and the undermining of the open internet norms are also highly relevant.

The institutional system to facilitate and regulate these dynamics is still in a dire need of improvement. The WTO JSI languishes, the IGF has no binding authority, and the multilateral rules on data flows are non-binding and are not widely respected. As various technological, regulatory and geopolitical path dependencies grow more entrenched, the window of opportunity to create successful global digital governance is closing. Sovereignty in today's digital age is not outdated or absolute, but contested, hybrid and a constant subject of negotiation, and is becoming increasingly significant in the granting and withholding of economic, political and security powers in the international system. The challenge at the heart of this issue is creating governance structures that can keep the national legality alive without losing the cooperative potential of a globally interoperable digital commons, the most powerful force of human knowledge, economic productivity and political communication ever created.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

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.
- Budnitsky, S. (2017). Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace. *International Journal of Communication*, 11, 5-5.
- Bai, Y. (2026). Digital Geopolitics and the Governance of Cross-Border Data Flows. *Journal of Sociology and Education*, 2(1).
- Bradford, A. (2020). The Brussels effect: How the European Union rules the world. *Oxford University Press*.
- Chari, S. G. (2025). Power, pixels, and politics: the geopolitics of emerging technologies in the digital age. *London Journal of Research in Humanities and Social Sciences*, 25(2), 1-99.
- Development (UNCTAD) (2024). Digital economy report 2024: shaping an environmentally sustainable and inclusive digital future. *Stylus Publishing, LLC*.
- Fratini, S., Pohle, J., Di, M. D., Thabit, G. S., & Sgueo, G. Digital Sovereignty as a Geopolitical Strategy.
- Falencik, M. I. (2021). The Internet in Everything: Freedom and Security in a World with No Off Switch. *International journal of communication (Online)*, 1154-1157.
- Franken, J., Reinhold, T., Dörnfeld, T., & Reuter, C. (2025). Hidden structures of a global infrastructure: Expansion factors of the subsea data cable network. *Technological Forecasting and Social Change*, 215, 124068.
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International security*, 44(1), 42-79.
- Gennari, P. (2024). Data equity and official statistics in the age of private sector data proliferation. *Statistical Journal of the IAOS*, 40(4), 757-764.
- Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômout, C., ... & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, 28(2), 919-958.
- ITU (2024). Global Cybersecurity Index 2024.
- Jansen, B., Kadenko, N., Broeders, D., Van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 101862.
- Jose, R., & Kaukab, R. S. (2024). WTO Joint Initiative on E-Commerce State of Play.
- Kovalevskaia, N. V., Tikhotskaia, M. A., & Shevchenko, Y. N. (2021). "Digital Geopolitics" in the Regional Context: Challenges and Prospects of the European Union on its Way towards Information Sovereignty. *Мировая политика*, (4), 52-65.
- Keohane, R. O., & Nye Jr, J. S. (1973). Power and interdependence. *Survival*, 15(4), 158-165.
- Laine, J. P. (2026). Beyond territorial discontents: the surprising persistence of borders in a fragmented world. *Space and Polity*, 30(1), 43-53.
- Li, J. (2026). Governing high-risk technologies in a fragmented world: Geopolitical tensions, regulatory gaps, and institutional barriers to global cooperation. *Fudan Journal of the Humanities and Social Sciences*, 19(1), 113-137.
- Mayer, M., & Nock, P. J. (2025). Digital fragmentations, technological sovereignty and new perspectives on the global digital political economy. *Global political economy*, 4(1), 2-13.
- No, P. Rethinking Sovereignty in the Digital Age: The Impact of Information Systems on National Borders and Authority. Organization for Economic Co-operation and Development (2019). *Going digital*:

Shaping policies, improving lives.

- Papyshev, G., & Chan, K. J. D. (2026). AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities. *Electronic Markets*, 36(1), 8.
- Rydning, D. R. J. G. J., Reinsel, J., & Gantz, J. (2018). The digitization of the world from edge to core. Framingham: *International Data Corporation*, 16, 1-28.
- Rahman, A. (2025). The Digital Silk Road: a strategic initiative in China's multifaceted superpower quest. *Asian Journal of Political Science*, 33(3), 529-549.
- Sohrbeck, Anna Junker, Shi Yadong, and Jesper Willaing Zeuthen. "Global Data Governance: The Global Fragmented Data Regulatory Framework and Digital Technology's Role in International Relations Theory." (2023).
- Seong, J., White, O., Woetzel, J., Smit, S., Devesa, T., Birshan, M., & Samandari, H. (2022). Global flows: The ties that bind in an interconnected world. *The McKinsey Global Institute Discussion Paper*.
- Soomro, M. A., Memon, M. S., & Bukhari, N. S. (2019). Impact of stress on employee's performance in public sector universities of sindh. *Sukkur IBA Journal of Management and Business*, 6(2), 114-129.
- Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, 44(8), 102003.
- Tan, J. (2026). Public AI and the Architecture of Sovereignty. Open for Debate: Governance, Power, and the Limits of Internet Openness, 148.
- Werthner, H., Ghezzi, C., Kramer, J., Nida-Rümelin, J., Nuseibeh, B., Prem, E., & Stanger, A. (2024). Introduction to digital humanism: A textbook (p. 637). *springer nature*.
- World Bank Group (2016). World development report 2016: Digital dividends. *World Bank Publications*.
- Xiong, W., Wu, D. D., & Yeung, J. H. (2025). Semiconductor supply chain resilience and disruption: insights, mitigation, and future directions. *International Journal of Production Research*, 63(9), 3442-3465.
- Yılmaz, C. (2026). The Geopolitics of Artificial Intelligence: Power, Regulation, and Global Governance. *UFÜ Sosyal ve Beşeri Bilimler Dergisi*, 2(3), 39-70.
- Yusuf, M., Rafli, M., & Rahmat, R. (2026). Reassessing State Sovereignty in the Era of Global Digital Governance. *International Legal Dimension Journal*, 1(1), 49-60.