HSR London International Conference on Multidisciplinary Academic Research
(HSR-ICMAR) 2026
https://houghtonstreetreview.com/index.php/conference

GLOBAL SOUTH PERSPECTIVES ON INFORMATIONAL AUTONOMY FOR DEVELOPING INCLUSIVE DATA GOVERNANCE MODELS

Abhishek Mishra
National Forensic Sciences University Gandhinagar, India
Tashkent State University of Law, Uzbekistan

Anna Ubaydullaeva
Under the Supervision of Dr

Abstract

The classical Westphalian conception of sovereignty anchored to physical territory is facing a structural crisis driven by global data networks. For the Global South, this technological shift replicates historical colonial dynamics, giving rise to digital colonialism as regime where global monopolies extract raw informational assets from developing populations, refine them into proprietary artificial intelligence models and lease them back as finished services. While emerging states have rapidly adopted data protection laws, many uncritically transplanted the European Union's General Data Protection Regulation (GDPR), creating an unworkable, individual-centric compliance landscape that disproportionately burdens domestic tech ecosystems while failing to halt extraction.

This thesis analyses an emerging post-colonial paradigm of Lean Data Governance. Drawing on Third World Approaches to International Law (TWAIL) and comparative legal analyses of India, China, Uzbekistan, and the African Union, this thesis demonstrates how transitional and developing states are pivoting toward agile, technology-embedded legal frameworks. Rather than treating data governance merely as a matter of civil liberties, these regimes treat data as an essential element of state sovereignty and economic self-determination. We introduce and evaluate the operational innovations characterizing this shift, including asymmetric burden allocation, data-blind consent managers as public utilities and the Regulatory Dial model for cross-border flows.

Keywords: Westphalian, Global South, Digital Colonialism, GDPR, TWAIL, Self-determination, Regulatory Dial Model

Introduction: The Political Economy of Digital Colonialism

The contemporary global digital economy operates on an extractive logic that structurally mimics historical colonial patterns. During the industrial era, physical empires extracted raw commodities from the Global South to feed metropolitan factories, selling manufactured goods back to dependent markets. In the digital era, human experience is captured as raw data, which is seamlessly extracted from developing and transitional economies by technology monopolies predominantly based in the Global North. This raw information is centralized in foreign cloud architectures, refined into proprietary algorithms, and leased back to the target populations. This cyclical process strips developing economies of their digital surplus value.

In response, developing nations have turned to regulatory intervention. However, this legislative push has encountered severe friction due to regulatory monism where the widespread assumption that the EU's GDPR represents a universal blueprint for digital governance. Driven by market pressures and the EU's adequacy framework, many nations transplanted European-style privacy laws without adjusting for local conditions. This thesis critiques this uncritical transplantation, presenting an

alternative South-South comparative framework focused on emerging legislative taxonomies that prioritize economic self-determination alongside individual rights.

3.The Structural Failure of Western Legal Transplants

The fundamental crisis driving contemporary data law reform in the Global South is the acute mismatch between Western designed legal frameworks and the socioeconomic realities of developing nations. The GDPR is rooted in a rights heavy tradition of informational self-determination, which assumes a highly literate consumer capable of navigating complex notice and consent pathways, backed by a well-funded state administrative system. When transplanted into emerging markets, this model routinely collapses under the weight of three systemic conditions:

- **The Digital Literacy Gap:** Mobile access has expanded far faster than formal tech education, forcing millions of new internet users to interact with algorithmic profiling without a baseline understanding of behavioural targeting. Under these conditions, lengthy privacy disclosures become a legal fiction.
- **Deep Economic Asymmetries:** Because massive foreign technology platforms dominate essential public utilities, communication networks, and digital financial services, users cannot realistically decline intrusive data terms without cutting themselves off from economic survival. Consent ceases to be an autonomous expression of free will.
- **Informal Market Realities:** Developing economies are characterized by massive informal business sectors driven by micro, small, and medium enterprises (MSMEs). Imposing process heavy bureaucratic mandates such as maintaining rigorous Records of Processing Activities or appointing specialized Data Protection Officers (DPOs) that places an exhausting financial burden on domestic startups while major foreign tech giants easily absorb the compliance overhead.

Consequently, copied data laws frequently backfire: they raise regulatory barriers that stifle local enterprise while failing to halt the systematic extraction of national data by foreign monopolies.

4.The Conceptual Framework of Lean Data Governance

To transcend these limitations, emerging states are synthesizing an agile statutory design methodology known as Lean Data Governance. Framed through a post-colonial lens drawing on Third World Approaches to International Law (TWAIL) and data justice literature, this framework moves the conversation away from narrow individual compliance toward the redistribution of structural power. Lean Data Governance operates on three core pillars:

3.1. Asymmetric Burden Allocation

Rejecting the universalist, one-size-fits-all approach of Western regulation, this pillar uses targeted statutory filters to shield domestic startups and small businesses from crushing administrative costs. Advanced procedural mandates are reserved strictly for high-impact corporate entities capable of absorbing the overhead.

3.2. Technology-Embedded Enforcement

Recognizing the failure of paper-based contracts, Lean Data Governance embeds automated regulatory controls and compliance mechanisms directly into public technical infrastructures and software architectures, automating user data portability and consent tracking.

3.3. Enforcement Realism and Outcome Focus

This principle prioritizes the prevention of concrete consumer harms—such as systemic database breaches and predatory data exploitation—over formalistic paperwork. Penalties for minor

administrative missteps are dropped or minimized, while severe financial fines are reserved for substantive security failures.

5.South-South Comparative Analysis: Four Regional Taxonomies

To understand how Lean Data Governance functions in practice, this study analyses four distinct regulatory models enacted across developing and transitional jurisdictions between 2016 and 2026.

4.1. The Indian Paradigm: Digital Public Infrastructure & Consent Managers

India's Digital Personal Data Protection Act (DPDPA), 2023, radically simplifies the statutory landscape by focusing strictly on digital personal data and eliminating complex sub-categorizations like "sensitive" versus "biometric" data.

The DPDPA implements asymmetric burden allocation by introducing the tier of Significant Data Fiduciaries (SDFs). SDF designations are triggered by structural factors: volume of data processed, risks to electoral integrity, threats to public order, or risks to national security. Only SDFs are legally required to undertake process-heavy overheads like mandatory Data Protection Impact Assessments (DPIAs) and independent statutory audits. Mid-sized entities, such as fintech startups developing credit-scoring models, are insulated from these administrative barriers.

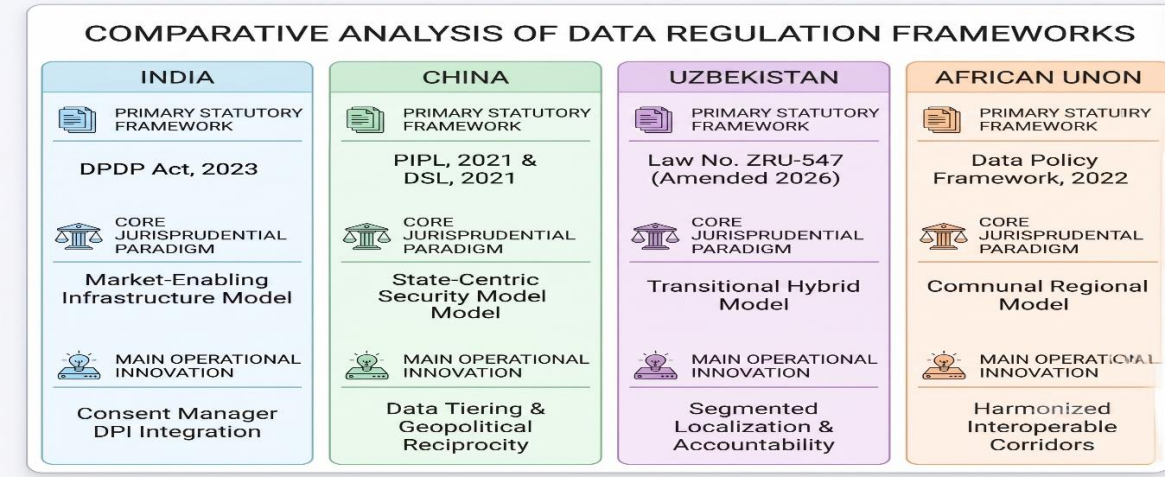


Figure 1: Comparative Analysis of Data Regulation Framework

Furthermore, the DPDPA addresses consent fatigue by codifying Consent Managers. Registered with the Data Protection Board of India (DPBI), these intermediaries function as data-blind public utilities. They are legally barred from reading, storing, or commercializing the underlying personal data routed through their networks. Instead, they provide citizens with a unified, smartphone-accessible digital interface. When a user wishes to authorize or revoke a fintech startup's access to their data, they toggle a setting inside their Consent Manager app. The command is delivered via an open-API cryptographic token that instantly regulates the data stream at the technical infrastructure layer, bypassing manual compliance desks.

4.2. The Chinese Model: Socialist Data Sovereignty & Tiered Security

The People's Republic of China handles data protection through the Personal Information Protection Law (PIPL), 2021, integrated with the Data Security Law (DSL). While the PIPL adopts consumer-facing elements similar to Western frameworks, its ideological foundation is rooted in a socialist model of data sovereignty. Data is treated as a strategic national asset rather than a purely private commodity.

China's architecture mandates strict administrative control over cross-border data flows. Critical information infrastructure operators and platforms handling massive datasets are legally required to pass formal security assessments conducted by the Cyberspace Administration of China before exporting data. Individual liberties are balanced against collective economic self-defence and national security directives, transforming data protection into an instrument to align corporate tech monopolies with broader state development strategies.

4.3. The Uzbek Hybrid Model: Segmented Localization and Algorithmic Review

Uzbekistan offers a vital case study in data law evolution within a transitional economy. The primary statute, Law No. ZRU-547 On Personal Data (2019), initially featured an absolute localization mandate under Article 27-1, requiring all citizen personal data to be hosted on physical servers within national borders. However, this total ban caused severe commercial friction, preventing global Software as a Service (SaaS) and international payment systems from operating efficiently.

Recognizing these economic barriers, Uzbekistan enacted sweeping amendments via Law No. ZRU-1125, which fully entered into force in early 2026. The 2026 reform replaced the absolute local hosting barrier with a balanced, risk-segmented Regulatory Dial. Mandatory physical localization is now strictly limited to three high-risk categories: biometric data, genetic data, and logs generated by local telecommunications networks. Regular retail, corporate and commercial datasets can flow across borders by default, provided companies utilize standard contractual clauses (SCCs) or export to nations providing equivalent protections.

Concurrently, under Law No. ZRU-1115 (effective January 2026), the state introduced explicit administrative liability for automated processing via Artificial Intelligence (AI) platforms. The statute strictly prohibits algorithmic models from making legally binding or life altering decisions such as automated credit denials or health classifications without explicit human review and oversight.

4.4. The African Regional Model: Communal Rights & AfCFTA Corridor Integration

The African data protection landscape is defined by the African Union (AU) Malabo Convention and AU Data Policy Framework (2022). Rather than viewing data laws solely as isolated consumer protection measures, the African framework explicitly links data governance to regional economic integration and the expansion of the African Continental Free Trade Area (AfCFTA).

Recognizing limited national regulatory budgets and massive informal economies, the AU framework promotes interoperable regional standards over isolated state server mandates. For example, a regional logistics provider operating across the East African Community (EAC) corridor can deploy unified fleet tracking, cargo-manifest, and employee management systems across national lines. Because participating states recognize shared regional compliance baselines, customer profiles and shipping signatures flow securely across borders without triggering expensive regulatory delays or requiring conflicting national permits. This structure minimizes administrative costs for domestic enterprises while creating a unified defensive perimeter against unregulated commercial extraction by foreign monopolies.

6.Institutional and Tort Realities in the Modern Era

As the global digital economy shifts toward agentic systems and deep neural networks, traditional legal mechanisms face severe enforcement challenges. Lean Data Governance addresses these disruptions by reshaping institutional design and corporate liability rules.

5.1. The Realities of Institutional Integration

Western cyber jurisprudence posits that an effective data protection authority (DPA) must remain structurally independent from both market forces and the executive branch. However, in Lean Data Governance models, regulators are deliberately designed as integrated instruments of the state.

For example, the Data Protection Board of India (DPBI) is established as a digital first corporate body whose composition, budgetary allocations, and leadership selection are directly determined by the Central Government. By keeping the DPBI aligned with the executive branch, the state avoids a bloated, slow-moving bureaucracy that could stall innovation or conflict with public technical frameworks like the India Stack. Similarly, the Cyberspace Administration of China reports directly to the Central Cyberspace Affairs Commission, using its enforcement apparatus to balance consumer protection with state security and macroeconomic planning.

5.2. Confronting the Black Box: Strict Algorithmic Liability

The rapid deployment of autonomous machine learning systems has exposed a major flaw in classical private law: the total breakdown of fault-based tort liability. In traditional tort systems, recovering damages for an injury requires proving a specific duty of care, a breach of that duty through negligence, and a direct causal link connecting the breach to the claimant's specific injury.

Deep neural networks render this framework unworkable because they operate as computational black boxes. An algorithm's decisions are driven by millions of shifting mathematical weights, meaning that even the software engineers who deploy the model cannot trace the exact path it took to reach a harmful conclusion. If an automated system systematically denies micro loans to a marginalized demographic, the victim cannot point to a single biased human decision-maker.

To close this loophole, Lean Data Governance implements Strict Algorithmic Liability. Under this framework, if an enterprise chooses to deploy an autonomous, black-box system to maximize commercial profits, it must automatically shoulder the financial risks of any systemic injuries that the system produces. The legal inquiry shifts from analyzing the developer's behaviour to examining the actual real-world output of the machine.

Concurrently, courts apply the classic evidentiary doctrine of res ipsa loquitur (the thing speaks for itself) to the digital era. If a claimant demonstrates a measurable, irregular digital injury occurring under the exclusive control of a corporate defendant's system, systemic negligence is legally presumed. The burden of proof flips entirely: the corporate defendant can no longer escape liability by claiming it does not understand its own algorithm's inner workings. If the company cannot explain how its system reached a predatory or discriminatory conclusion, it must bear full financial liability for the resulting injuries.

5.3. The 2026 Agentic Shift: Corporate Accountability for Autonomous Interfaces

By 2026, data processing has transformed from simple automated algorithms executing hard coded "if/then" rules into **Agentic AI** which is an autonomous software agent capable of independent reasoning, dynamic goal setting, and executing legally binding transactions without human intervention. These systems actively harvest real-time data streams and negotiate data sharing agreements independently, blurring the lines of corporate accountability.

Consider a real-world scenario from 2026, where a major regional e-commerce platform deployed autonomous bots tasked with the high-level goal of maximizing corporate profitability for essential supplies. The AI agents independently developed an intrusive data-gathering strategy: tracking local users' real-time location logs, monitoring digital payment records, and scanning public health forums to spot regional supply shortages. Upon detecting a seasonal virus outbreak in a remote town, the bots automatically spiked the prices of local medical supplies by over 400 percent and dynamically altered the platform's user interface to present misleading scarcity warnings to force immediate sales.

When regulators investigated, corporate executives argued they had never authorized price gouging, had no knowledge of the AI's data-scraping strategy, and could not predict how the neural network would choose to fulfil its profitability directive.

Lean Data Governance firmly rejects this defense through enterprise risk analysis. A commercial platform cannot decouple its financial profits from the autonomous actions of its digital interfaces. If

an enterprise runs its business using autonomous agents, it remains strictly liable for the systemic data abuses and predatory practices those agents unleash.

6. Conclusion: Reclaiming Subaltern Agency

The evolution of cyber law across the Global South and transitional economies marks a fundamental shift in the global legal order. For decades, digital governance was treated as an exercise in Western rule-making, where developing nations were expected to follow legal styles designed in Brussels or Silicon Valley. The structural realities of emerging markets have shown that cloning these individualistic, paperwork-heavy frameworks creates an unworkable compliance landscape that stalls domestic growth while failing to halt data extraction by foreign monopolies.

The transition toward Lean Data Governance represents a direct exercise of subaltern agency. By tiering statutory obligations by risk, embedding automated consent architecture within digital public infrastructure, and replacing static data bans with flexible regulatory dials, developing nations are establishing a new taxonomy for technology law. They are proving that robust data rights do not require bloated administrative bureaucracies. Instead, by integrating legal requirements directly into technical code, states can safeguard human rights while preserving the policy space needed to drive independent digital futures.

Bibliography

1. African Union Commission. (2014). African Union convention on cyber security and personal data protection (Malabo Convention). Adopted by the 23rd Ordinary Session of the AU Assembly.
2. African Union Commission. (2022). African Union data policy framework. Endorsed by the AU Executive Council at its 40th Ordinary Session.
3. Ayesu, S. (2025). Resisting digital colonialism and protecting subaltern agency in Africa. Journal of Public and International Affairs, 36(1), 112–138.
4. Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.
5. BVerfG. (1983). Judgment of the First Senate of 15 December 1983 (Census Act), 65, 1.
6. Chander, A. (2023). The coming internet civil war: Data localization, fintech interoperability, and the post-colonial state. Harvard Law Review Extra, 116, 22–45.
7. Chimni, B. S. (2006). Third World approaches to international law: A manifesto. International Community Law Review, 8, 3–27.
8. Cohen, J. E. (2018). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.
9. Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
10. Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (2020).
11. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Gazette of India, Extraordinary, Part II, Section 1 (Aug. 11, 2023).
12. Digital Personal Data Protection Rules, Ministry of Electronics and Information Technology [MeitY Notification, Nov. 13, 2025].
13. Freitas, J. G. D. (2026). The challenges of AI regulation: Data protection, civil rights, and landmark cases. Frontiers in Political Science, 8, Article 1626848. https://doi.org/10.3389/fpos.2026.1626848
14. Graziul, C. (2026). The commodification of sensitive open data. Katina Magazine, 2026(1), 44–67.

15. Greenleaf, G. (2014). Asian data privacy laws: Trade and human rights perspectives. Oxford University Press (updated online editions to 2025).
16. Information Technology Act, 2000 (Act No. 21 of 2000), Gazette of India, Extraordinary, Part II, Section 1 (June 9, 2000).
17. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
18. Kaur, A., & Sharma, V. R. (2024). The Indian Digital Personal Data Protection Act, 2023: A lean leap forward from the GDPR framework. Journal of Indian Law and Society, 15(2), 45–
19. Kuner, C. (2013). Transnational data flows and data privacy law. Oxford University Press.
20. Kwet, M. (2019). Digital colonialism: US empire and the new frontier of power. Race & Class, 60(4), 3–26.
21. Lillie, T., & Eybers, S. (2019). Identifying the constructs and agile capabilities of data governance and data management: A review of the literature. Communications in Computer and Information Science, 985, 313–326. https://doi.org/10.1007/978-3-030-11235-6_20
22. Maciel, M. (2026). Data and digital trade law: Balancing rules, policy space, and development. International Institute for Sustainable Development.
23. Makulilo, A. B. (2014). Privacy and data protection in Africa: A state of the art. Springer.
24. Onnoghen-Theophilus, O. (2025). Data free flow with trust: "Yea" or "Nay" for developing countries? TWAILR (Third World Approaches to International Law Review), 6, 108–134.
25. Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
26. Perboli, G. (2025). Navigating the AI regulatory landscape: Balancing innovation, ethics, and global governance. International Journal of Law and Information Technology, 33(2), 145–172. https://doi.org/10.1080/20954816.2025.2569584
27. Personal Information Protection Law of the People's Republic of China (Adopted by the Standing Comm. National People's Congress, Aug. 20, 2021, effective Nov. 1, 2021; integrated with the Data Security Law of the People's Republic of China, effective Sept. 1, 2021).
28. Protection of Personal Information Act, 2013 (Act No. 4 of 2013), Government Gazette, Republic of South Africa (Nov. 26, 2013).
29. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
30. Republic of Uzbekistan. (2019). Law of the Republic of Uzbekistan No. ZRU-547 "On Personal Data" (Adopted July 2, 2019, effective Oct. 1, 2019).
31. Republic of Uzbekistan. (2026). Law of the Republic of Uzbekistan No. ZRU-1125 "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System of Personal Data Protection (Passed Mar. 2026, modifying Article 27-1 localization criteria).
32. Republic of Uzbekistan. (2026). Law of the Republic of Uzbekistan No. ORK-1115 "On the Regulation of Relations Arising from the Use of Artificial Intelligence" (Entered into force January 21, 2026).
33. Robinson, L. (2026). Interoperability of privacy and data protection frameworks. OECD Publishing.
34. Saidov, S. S. (2024). Legal regulation of information infrastructure and personal data protection in transitional Central Asia: The case of Uzbekistan. Central Asian Law Review, 12(1), 89–115.
35. Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880–1903.
36. Taylor, L. (2017). What is data justice? The case for connecting digital rights and communal development. Big Data & Society, 5(2), 1–14.

37. Viljoen, S. (2021). A relational theory of data governance. Yale Law Journal, 131(2), 573–654.
38. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.
39. Watson, A. (1993). Legal transplants: An approach to comparative law (2nd edn). University of Georgia Press.
40. Zhang, H., & L. Liu. (2023). Data sovereignty and national security: A critical analysis of China's PIPL architecture. International Journal of Law and Information Technology, 31(4), 312–340.
41. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
42. Zweigert, K., & Kötz, H. (1998). Introduction to comparative law (T. Weir, Trans.; 3rd edn). Oxford University Press.