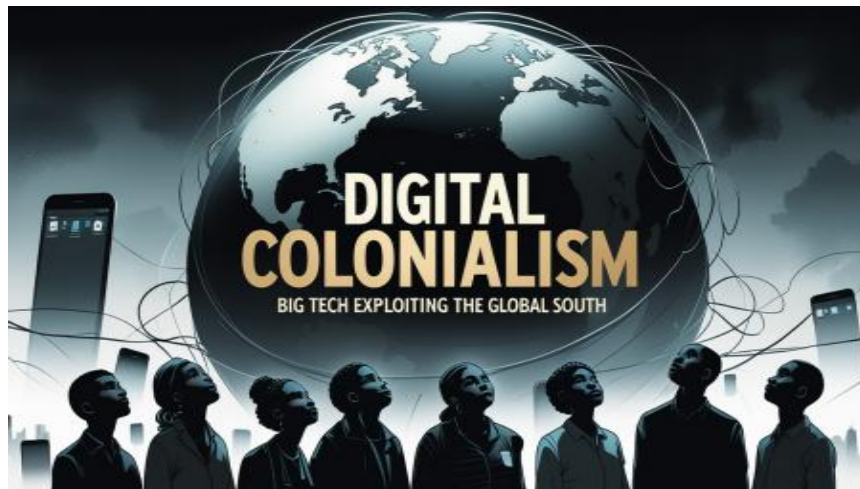


Digital Colonialism: The Struggle for Data Independence in the Global South

Mohosina Mostofa Mity¹

Introduction

In today's world, power is no longer measured only by territory, manpower, or military strength. It is increasingly defined by who controls information, who extracts value from it, and who decides how that information will shape societies. For many countries in the Global South, this new reality has unfolded quietly but decisively. Every digital transaction, health record, biometric scan, or social media interaction now travels through systems largely owned and governed by a handful of powerful corporations and foreign governments. What appears as progress on the surface often masks a deeper dependency—one that echoes older patterns of external control, only updated for the digital age.



Source: Computer Geek

¹Mohosina Mostofa Mity is a Research Associate at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the Bangladesh University of Professionals (BUP).

This emerging imbalance is described by many scholars as a form of digital colonialism: the concentration of data, platforms, and technological infrastructure in the hands of actors who sit far away from the people whose information they collect. The result is an unsettling shift in authority. Nations that fought long and hard for political and economic sovereignty now face a new struggle—protecting the autonomy of their data, the privacy of their citizens, and the integrity of their digital futures.

The Global South stands at a moment when choices about cloud services, cybersecurity, artificial intelligence, and digital governance will determine far more than efficiency or convenience. These decisions will shape who sets the rules of development, who benefits from innovation, and whose interests define the digital order. The fight for data independence has therefore become not just a technological concern, but a defining political and strategic challenge of our time.

Foreign Cloud Dominance and the Risks of Outsourced Sovereignty

Foreign cloud dominance has become a structural vulnerability for many states in the Global South. Today, a small number of global providers — led by Amazon, Microsoft and Google — control a majority share of the enterprise cloud market, concentrating computing power, storage, and the business logic that sits above raw data.² This market concentration means that critical national functions — from tax administration to health records, financial services, and emergency communications — increasingly depend on platforms and operators beyond domestic control.

The implications are both economic and political. Economically, reliance on external cloud services channels subscription revenues and long-term operational profits to foreign firms, while episodic outages or commercial disputes can disrupt public services. Politically, data hosted and processed on foreign infrastructure can be subject to legal regimes and government requests in the provider's home jurisdiction, weakening national control over sensitive information and intelligence. Attempts to reduce these risks through data localization laws or new domestic

²Haranas, Mark. 2025. "Global Cloud Market Share Q3 2025: AWS Lowers, Microsoft and Google Stay Same." Crn.com. 2025. <https://www.crn.com/news/cloud/2025/global-cloud-market-share-q3-2025-aws-lowers-microsoft-and-google-stay-same?>

regulation have been uneven in effect: some nations have managed partial repatriation of data flows, while others confront capacity gaps and high costs.³

Practical constraints also matter. Many countries lack the scale, reliable power, fiber connectivity, and skilled workforce needed to build and operate secure, competitive data centres. Recent regional surveys show rapid but nascent growth in African data-centre capacity, with markets still small relative to demand and dominated by a few large foreign entrants.⁴

A concrete case is Kenya. The success of mobile money and related services depended on fast, reliable platforms; Safaricom's investment in local cloud offerings illustrates an alternative model where regional providers develop local capacity to reduce foreign dependency and retain economic value.⁵ Yet even there, international cloud links remain essential for cross-border interoperability and for advanced services provided by global firms.

AI Dependency and Algorithmic Power Imbalances

The growing dependency on imported artificial intelligence systems creates serious power imbalances for countries in the Global South. Much of today's advanced AI infrastructure, including foundational models, compute power, and training data, remains concentrated in the Global North — giving companies and states from those regions disproportionate influence over how AI works and whose interests it serves. This dynamic is often described as a new form of “AI colonialism,” where external actors set the rules, while developing nations become consumers rather than creators.⁶

³ Karthika Rajmohan. 2025. “Data Localization: India’s Tryst with Data Sovereignty.” Tech Policy Press. January 23, 2025. <https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/>.

⁴ Africa Data Centres Association. *Africa Interconnection Report 2023*. Abidjan, Côte d’Ivoire: Africa Data Centres Association, 2023

⁵ “It’s in the Cloud, Simple.” 2024. Safaricom.co.ke. 2024. <https://newsroom.safaricom.co.ke/innovation/its-in-the-cloud-simple>.

⁶ Warganegara, Muhd Rafli Ramadhan. 2024. “Shifting from ‘AI Solutions’ to ‘AI Coloniality’: Resignification of Artificial Intelligence and Digital Apartheid.” *Global South Review* 6 (1): 7. <https://doi.org/10.22146/globalsouth.94333>.

One profound risk lies in algorithmic bias. Many AI models are trained on datasets drawn from Western contexts, using language, cultural assumptions, and societal patterns that do not translate well to the realities of African, Asian, or Latin American communities.⁷ For example, automated content moderation systems often fail in less-resourced languages like Swahili or Quechua, because the underlying models were not designed with those linguistic complexities in mind.⁸ This not only undermines inclusivity but also entrenches systemic inequities: communities become misrepresented, censored, or surveilled by technology that does not “see” them properly.



Source: Observer Research Foundation

In public sector uses, reliance on foreign AI raises sovereignty concerns. In Telangana, India, a facial-recognition-based system for pension authentication reached a reported 93 percent success rate in initial trials — but critics warn that this model was never adequately stress-tested for scale,

⁷ Adams, Rachel. 2024. “AI Is Bad News for the Global South.” Foreign Policy. December 17, 2024. <https://foreignpolicy.com/2024/12/17/ai-global-south-inequality>.

⁸ Shahid, Farhana, Mona Elswah, and Aditya Vashistha. 2025. “Think Outside the Data: Colonial Biases and Systemic Issues in Automated Moderation Pipelines for Low-Resource Languages.” ArXiv.org. 2025. <https://arxiv.org/abs/2501.13836>.

privacy, or ethical risks.⁹ Without strong national capacity to audit, adapt, or contest these systems, governments and citizens remain exposed to external control over highly sensitive data.

Moreover, the economic value of AI often flows outward, not inward. As resource-constrained African economies adopt AI, much of the investment, expertise, and platform value is supplied by foreign multinationals, making African countries dependent on external funding and technology.¹⁰ This can stifle the development of indigenous AI talent and institutions, perpetuating a cycle in which the Global South provides data and labor but captures only a fraction of the benefits.

Ultimately, this asymmetry threatens both justice and autonomy. Without deliberate policymaking, capacity-building, and infrastructure investment, countries in the Global South risk being locked into AI ecosystems that serve external priorities — reinforcing a digital hierarchy rather than dismantling it.

Cybersecurity Vulnerabilities and the Geopolitics of Data Access

Cybersecurity has become a frontline security concern for countries in the Global South, not only because digital systems are expanding rapidly, but because these systems are often built on fragile foundations. Many states now depend on foreign-made software, imported hardware, and external cloud platforms, creating an environment where vulnerabilities accumulate faster than they can be addressed. When critical infrastructure — from electricity grids to banking platforms — relies on technologies outside national control, the state’s ability to protect itself becomes limited. This dependence turns every cyber breach into a potential geopolitical incident, not just a technical failure.

The geopolitical stakes are high because cyberspace is no longer neutral territory. Major powers view data access as a strategic asset, and cyber intrusions have become subtle instruments of influence. In several developing countries, cyber incidents involving government ministries,

⁹ “AI Governance: The ‘Regulatory Bottleneck’ in the Global South.” 2022. Hertie School. 2022. <https://www.hertie-school.org/en/content/detail/content/ai-governance-the-regulatory-bottleneck-in-the-global-south>.

¹⁰ Frimpong, Victor. 2025. “Artificial Intelligence Investment in Resource-Constrained African Economies: Financial, Strategic, and Ethical Trade-Offs with Broader Implications.” *World 6* (2): 70. <https://doi.org/10.3390/world6020070>.

election systems, and financial institutions have revealed patterns of targeted surveillance and data extraction by external actors. These intrusions are rarely random; they often reflect foreign interest in political trends, resource negotiations, or military planning. When states cannot trace, deter, or retaliate against such attacks, they risk operating in a security environment shaped by others.

A key challenge is that many nations lack the skilled workforce and institutional capacity to audit foreign technologies or verify how data flows across borders. As a result, sensitive information — including communications metadata, biometric records, and trade data — may pass through systems where foreign governments can request access under their own legal frameworks. This creates an uneven playing field in which powerful actors can shape political outcomes without overt interference.

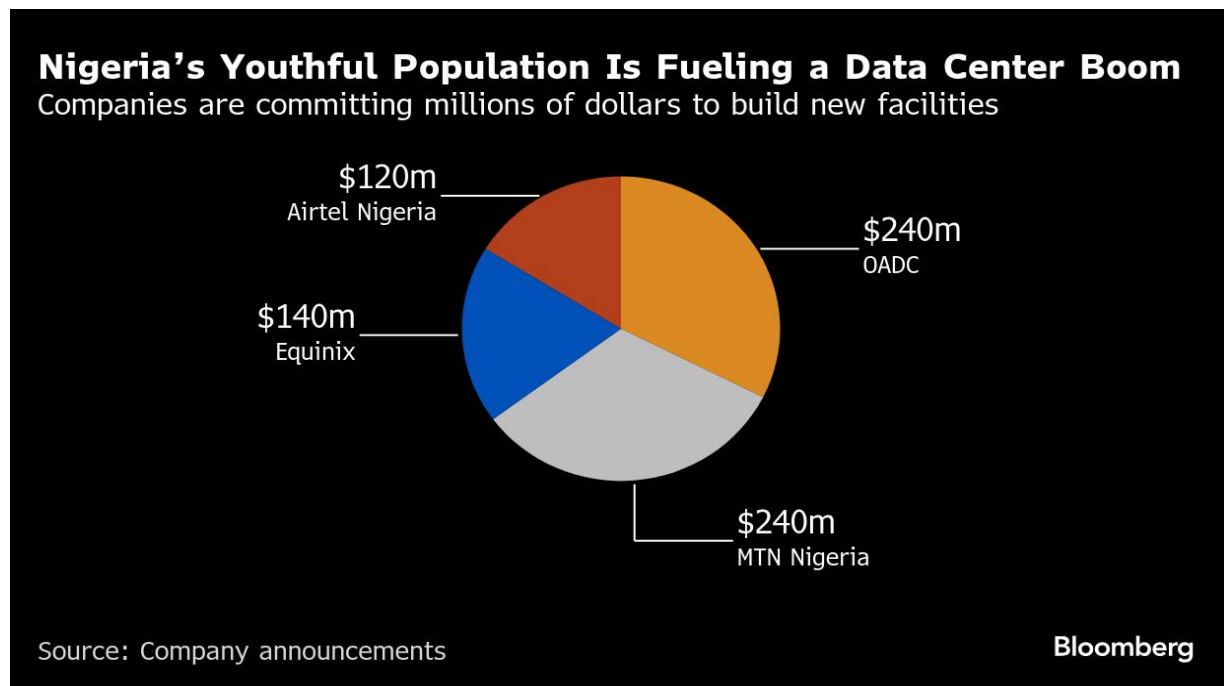
The Global South therefore faces a dual threat: technical exposure to cyberattacks and strategic exposure to foreign leverage. Reducing these risks demands long-term investment in national cyber agencies, domestic encryption capacities, and clear agreements on cross-border data flows. Without such measures, cybersecurity will remain an area where geopolitical pressure quietly overrides national sovereignty.

Regulatory Asymmetries and the Weak Bargaining Power of Developing States

One of the core challenges for developing countries in the digital age is regulatory asymmetry — the fact that their legal, institutional, and bargaining power is much weaker relative to global technology giants. While big tech firms operate globally with enormous resources, many governments in the Global South struggle to craft and enforce regulations that can protect their citizens' data and assert meaningful sovereignty. This imbalance is not purely technical; it reflects deeper structural inequalities rooted in regulatory capacity, fiscal constraints, and geopolitical leverage.¹¹

¹¹ “Data Protection Regulation in the Global South.” 2024. Carnegie Endowment for International Peace. 2024. <https://carnegieendowment.org/posts/2024/02/data-protection-regulation-in-the-global-south>.

A striking example from 2025 comes from **Nigeria**, which demanded that Google, Microsoft, and Amazon concretely commit to building data centers on Nigerian soil.¹² Despite repeated promises, the tech giants had delayed investment, prompting Nigerian authorities to set up a working group with these companies. Nigeria’s regulator explicitly warned that waivers would no longer be tolerated — it was time for concrete roadmaps or local providers would be used instead.



Source: Energy Connects

This case reveals exactly how weak bargaining power can manifest. On one hand, Nigeria has publicly stated the importance of data being stored locally to protect its citizens’ information and to foster economic value within the country. On the other hand, global tech companies argue that local infrastructure does not meet their technical requirements, or that the investments are too risky without more favorable regulatory terms. The imbalance is exacerbated by long-term contracts, high costs of establishing sovereign infrastructure, and limited local alternatives.

Beyond Nigeria, many developing states face similar challenges in data protection and cross-border data flows. Their regulatory frameworks may be less mature, capacity to enforce global

¹² “Data Protection Regulation in the Global South.” 2024. Carnegie Endowment for International Peace. 2024. <https://carnegieendowment.org/posts/2024/02/data-protection-regulation-in-the-global-south>.

firms' compliance may be limited, and legal systems can be ill-prepared to negotiate complex technology deals. As a result, countries risk being dependent on Big Tech for the storage, processing, and monetization of their own citizens' data — reinforcing a structural imbalance where global firms gain value, while national governments struggle to assert control.

Building Indigenous Tech Ecosystems: The Path to Digital Self-Reliance

Building indigenous tech ecosystems is the most durable route to digital self-reliance. Local capacity reduces external rent extraction, keeps value within the economy, and strengthens control over sensitive systems. Practical progress can be seen across several cases.

Kenya demonstrates a regional model where a dominant telecom firm has deliberately expanded into platforms, cloud services, and digital financial infrastructure. Safaricom's investments in local technology and ecosystem support have helped retain more economic value domestically and foster a pipeline of startups that leverage regional infrastructure rather than exporting all activity to foreign clouds.¹³ This approach has supported resilience in payments and public services.

India offers a scale example: massive private and public investment into data centres and AI-ready infrastructure has attracted tens of billions in commitments and created local capacity for advanced services. Between 2019 and 2024 India drew roughly US\$60 billion in data-centre investment commitments, signaling how concentrated, coordinated investment can change a country's bargaining position with global platforms.¹⁴

Smaller economies can still succeed by combining policy clarity, incentives, and targeted partnerships. Rwanda's deliberate build-out of digital public goods, skills programs, and investor facilitation has helped incubate local innovators and anchor some regional services domestically — a reminder that political will and coherent strategy matter more than size alone. But challenges still remain. The Nigeria cloud market, for instance, is still small relative to demand (estimated at

¹³ "ACCELERATING DIGITAL INCLUSION 2024 SUSTAINABLE BUSINESS REPORT." n.d.
<https://www.safaricom.co.ke/images/Downloads/Safaricom-Sustainable-Report-2024-compressed.pdf>.

¹⁴ "India's AI-Powered Data Centre Boom - \$100 Billion Investment Forecast by 2027: CBRE." 2024. IndiaAI. 2024.
<https://indiaai.gov.in/article/india-s-ai-powered-data-centre-boom-100-billion-investment-forecast-by-2027-cbre>.

about US\$1.03 billion in 2025) and faces currency and infrastructure constraints that make indigenous scale costly.¹⁵

Policy lessons are clear. Governments should combine demand-side measures (preferential public procurement, sovereign cloud initiatives), supply-side support (incubators, tax breaks, power and connectivity improvements), and international cooperation for technology transfer. When applied together, these steps convert scattered projects into coherent ecosystems that deliver both prosperity and sovereignty.

Bangladesh's Search for a Secure Digital Identity

Bangladesh's struggle for digital sovereignty has entered a decisive phase. In 2025, the government moved rapidly to reform the regulatory environment, introducing the Personal Data Protection Ordinance and a new Cyber Security Ordinance intended to protect sensitive data and strengthen national resilience.¹⁶ These measures signal a growing recognition that data flows are now intertwined with national security. Yet critics note that rapid drafting, limited stakeholder dialogue, and ambiguities within the laws risk weakening both public trust and long-term enforcement capacity. Strong legislation cannot function if institutions lack independence or the technical ability to monitor powerful actors.

The urgency is clear from recent cyber incidents. A surge of phishing campaigns at the start of 2025 targeted government agencies, law enforcement units, and academic institutions, exposing lingering gaps in digital hygiene. DDoS (Distributed Denial of Service) activity in late 2024 rose by over 100 percent, while a national audit reported that nearly one-third of government websites faced cyberattacks in the first half of 2024 alone.¹⁷ These numbers reflect a system that has

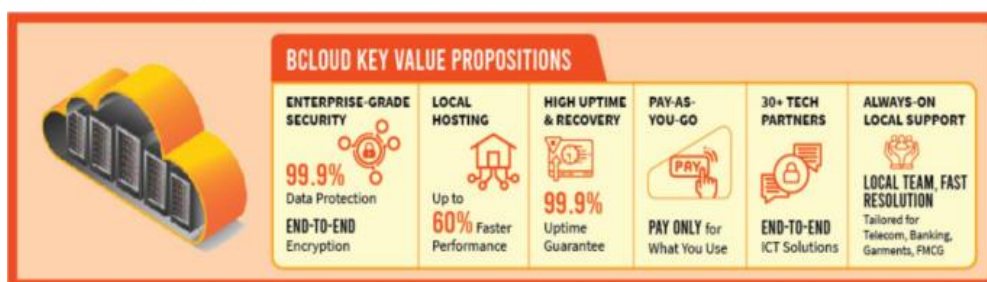
¹⁵ Mordor Intelligence. 2025. "Nigeria Cloud Computing Market Size & Share Analysis - Industry Research Report - Growth Trends." Mordorintelligence.com. 2025. <https://www.mordorintelligence.com/industry-reports/nigeria-cloud-computing-market>.

¹⁶ "The Daily Star." 2025. The Daily Star. October 9, 2025. <https://www.thedailystar.net/news/bangladesh/news/shielding-personal-data-govt-brings-big-tech-under-local-courts-purview-4006206>.

¹⁷ Bangladesh Cyber Security Intelligence. 2024. "DDoS Storm Hits Bangladesh: Cyberattacks Surge 105% - Bangladesh Cyber Security Intelligence (BCSI)." Bangladesh Cyber Security Intelligence (BCSI). November 8, 2024. <https://bcsi.gov.bd/ddos-storm-hits-bangladesh-cyberattacks-surge-105>.

expanded faster than it has secured, leaving public services vulnerable to foreign surveillance, criminal networks, and geopolitical manipulation.

On the infrastructure front, Bangladesh has taken meaningful steps. The Tier-IV data centre at Kaliakair has become a central node for public-sector digital services, and the partnership with Oracle Cloud Infrastructure aims to build a sovereign cloud environment where sensitive government data remain within national borders.¹⁸ Local initiatives such as Banglalink’s bCloud offer early examples of domestic cloud capacity, but these efforts must scale far more aggressively if the country hopes to avoid long-term dependency on foreign providers.¹⁹



Looking ahead, Bangladesh needs a deeper shift in ambition. It must treat data as a strategic national resource, not merely an administrative tool. This requires a dedicated sovereign data authority with real autonomy, a national open-source cloud initiative that reduces dependence on

¹⁸ “Bangladesh Data Center Company Limited (BDCCL).” 2025. Bdccl.gov.bd. 2025. <https://bdccl.gov.bd/site/page/0421bb87-0107-48be-814a-55980181fa5e/>.

¹⁹ “Banglalink BCloud: Driving Enterprise Digital Transformation.” 2025. The Business Standard. July 16, 2025. <https://www.tbsnews.net/features/panorama/banglalink-bcloud-driving-enterprise-digital-transformation-1189841>.

proprietary systems, and long-term investment in cyber-education to cultivate a generation of indigenous technologists. If Bangladesh pairs legal reform with genuine technological self-reliance, it can transform vulnerability into opportunity—emerging not as a passive consumer of digital systems, but as an architect of its own digital future.

Way Forward

The path toward data independence and digital self-reliance requires a combination of policy vision, technological investment, and societal engagement. For countries in the Global South, it is no longer sufficient to adopt technology developed elsewhere; they must actively shape the systems they depend upon. Building sovereign cloud infrastructure, for example, can provide governments and enterprises with control over critical data while fostering domestic innovation and creating economic value. Incentivizing local data centers, cloud services, and cybersecurity firms can reduce dependency on foreign providers and generate new jobs and expertise within the country.

At the same time, legal frameworks must be strengthened and harmonized with international standards. Data protection, cybersecurity, and AI governance laws should clearly define rights, responsibilities, and enforcement mechanisms, while also allowing flexibility to respond to emerging technologies. Enforcement is as important as legislation: independent agencies with technical capacity and institutional authority are essential to monitor compliance, audit foreign providers, and protect sensitive information from misuse.

Education and skill development form another critical pillar. Cultivating a workforce capable of developing, managing, and defending digital infrastructure ensures that technological sovereignty is not only theoretical but operational. Investments in AI research, open-source platforms, and cybersecurity education can create a domestic knowledge base capable of designing solutions suited to local needs, rather than relying solely on imported technologies.

International cooperation should complement domestic efforts. Strategic partnerships can enable technology transfer, knowledge sharing, and access to best practices without sacrificing sovereignty. By combining regulatory foresight, indigenous innovation, and selective collaboration, countries in the Global South can transform digital dependence into digital empowerment. For Bangladesh, and its peers, this approach offers the promise of converting data

from a source of vulnerability into a national asset, ensuring that the benefits of the digital revolution accrue to citizens, the economy, and the state, rather than to distant corporations or foreign governments.