



Repatriating East Africa's Data:

Reclaiming Control for
Sovereignty and Innovation

Author: Dorine Wanjeru-Kimathi
Date: November 2025

Executive Summary

In East Africa, much of the value generated from data produced by citizens, firms, and governments flows outward. Foreign companies and donor-led systems dominate the region's digital and data infrastructure, storing, processing, and monetising this data. The result is a modern form of dependence in which the region supplies raw data while others capture the profits and strategic advantages derived from it.

This issue is not simply a technological challenge but an economic and governance problem. When data on payments, agriculture, health, and education is hosted and analysed abroad, East African states lose opportunities to create jobs, tax revenue, and innovation capacity. They also lose visibility over their economies, compromising security and evidence-based policymaking.

The issue is not the use of global technology per se, but the lack of frameworks ensuring that the data generated within the region remains under its legal and economic control.

This brief argues that data sovereignty, the ability to govern, store, and use data according to regional priorities, is essential to the next phase of East Africa's digital transformation. Drawing on examples from Kenya, Tanzania, and Uganda, it shows how foreign-owned infrastructure, donor-driven platforms, and fragmented laws have entrenched structural dependency. It also illustrates how value is extracted through global cloud contracts, Fintech data models, and health information systems whose analytics and intellectual property are created elsewhere.



The brief proposes a set of pragmatic actions to reverse this trend:

1

Establish a binding regional data sovereignty framework that classifies data types, harmonises rules, and ensures collective jurisdiction.

2

Create sovereign and shared digital infrastructure, including EAC-owned data centres and a pilot “data embassy”.

3

Regulate external actors through a “trusted digital partner” certification for cloud and donor platforms.

4

Leverage international law to assert jurisdiction over submarine cables and ensure fair access for all member states.

5

Invest in regional capacity, data governance skills, analytics capability, and local innovation ecosystems to make sovereignty sustainable.

By repatriating and governing its data strategically, East Africa can build a resilient digital economy that serves its people first, strengthens regional integration, and positions it as a credible actor in global data governance debates.

1. Why Data Sovereignty Matters



Every mobile transaction, remote clinic record, school registration, and agricultural platform interaction produces information that fuels both local services and global analytics markets. Whoever controls that information determines how value is created, distributed, and taxed.

In the past decade, the region has made remarkable progress in digital inclusion, which has increased the volume of digital data. Mobile penetration exceeds 80% in Kenya and Tanzania; mobile money has reached even remote rural economies; and e-government portals are streamlining services^[1].

Yet these advances rest mostly on infrastructure and platforms owned or controlled outside the region. Cloud servers, analytics tools, and even some national databases are hosted abroad^[2], creating a dependence that limits self-determination.

Data sovereignty, therefore, is not a call for isolation. It is about ensuring that the data produced by East Africans contributes first to local development and innovation before fuelling profits elsewhere. It is about being able to set the terms of access and use, to retain a fair share of value, and to protect the rights and security of citizens.

[1] Communications Authority of Kenya, 'Sector Statistics Report Q4 2024-2025' (CA Report, September 2025) ;Tanzania Communications Regulatory Authority, 'Communications Statistics Report Quarter ending September 2025' (TCRA Report, October 2025)

[2] Yasin Tokat, 'The Big Tech versus the Nation-States: Clash of Economic Interests and Struggle to Compete on a Global Scale' (2023) SSRN Electronic Journal; Brookings Institution, 'Reducing Kenya's health system dependence on donors' (Brookings Article, 27 October 2021)

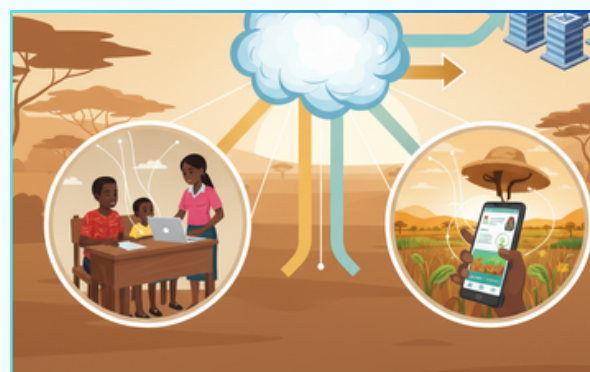
2. The Local Context: How Dependency Looks in Practice

2.1 Kenya – Digital Leadership Built on External Infrastructure

Kenya is a continental leader in digital services. The country's ICT sector contributes nearly 10% of GDP,^[3] and mobile money platforms process more than half of the transactions in this sector. Yet the foundations of this ecosystem are externally anchored. Most public digital platforms, including the flagship eCitizen portal, rely on foreign cloud hosting and proprietary software.^[4] In 2023, when a cyberattack temporarily disabled the platform, more than five thousand government services were disrupted, from passport applications to company registrations.^[5] The incident exposed how even a temporary loss of access to externally hosted systems can paralyse public functions.

Kenya's health information systems reveal a deeper layer of dependency. The country's health system is highly reliant on donor funding, particularly for critical programmes like HIV treatment. In some years, donor spending on health has been double that of the Kenyan government, and for every dollar the government spends on HIV programmes, donors contribute an additional USD 2.2million.^[6]

This financial dependency is directly mirrored in the digital systems used to manage these programmes. A significant portion of Kenya's health information infrastructure, which manages sensitive patient data, epidemiological trends, and resource allocation, is funded and often indirectly managed by international donors, such as the U.S. President's Emergency Plan for AIDS Relief (PEPFAR). This creates a 'shadow state' for critical national data. The resulting datasets containing sensitive public-health information are sometimes stored or mirrored on servers governed by donor agreements rather than national law. In practice, this means the state does not always have full custody or visibility over its own public data.



[3] Communications Authority of Kenya, 'Sector Statistics Report Q4 2024-2025' (CA Report, September 2025).

[4] 'The Role of the State and Foreign Companies in the Launch and Implementation of Digital Government Services in Kenya and Zambia – CIPIT' (Strathmore.edu2025).

[5] Carnegie Endowment for International Peace, 'When the Rubber Meets the Road: Cybersecurity and Kenya's Digital Superhighway' (Carnegie Report, October 2023).

[6] Brookings Institution, 'Reducing Kenya's health system dependence on donors' (Brookings Article, 27 October 2021).

The problem of digital dependencies extends to the region's physical infrastructure, particularly submarine cables. The issue is not the use of these cables, which are essential for global connectivity. The problem is the lack of sovereign governance. The majority of these cables and their landing stations are owned and operated by foreign entities, creating "chokepoints"

where data can be intercepted, accessed, or disrupted, all beyond the EAC's legal jurisdiction.^[7] This forces the region to effectively pay transit fees to foreign corporations to move its data over foreign-owned infrastructure. This data becomes subject to the legal and political jurisdiction of another country, undermining the very foundation of national security in the digital age.

2.2 Tanzania – Expanding Connectivity Without Control

Tanzania's rapid growth in internet use has created massive new datasets. The telecoms regulator reported over 730 petabytes of data consumed in just one quarter of 2025^[8]. Agricultural platforms now gather detailed information on farmers, yields, soil, and weather patterns; assets that could transform productivity if properly analysed and shared.

Yet many of these systems were introduced by development partners

or multinational agritech firms and not connected to an integrated national data platform. Data from smallholders, collected via mobile apps or satellite sensors, often feeds into proprietary analytics tools hosted abroad. The insights generated, such as market forecasts, credit scores, and supply-chain optimisations, are sold back to African institutions or global buyers.^[9] The farmers and governments that generated the data rarely see a direct share of the returns.

2.3 Uganda – Early Growth, Familiar Risks

Uganda's digital economy is expanding, with ICT already contributing 9% of GDP^[10]. The country has embraced digital health systems, digital ID, and edtech. But the pattern mirrors its neighbours:

critical systems, such as the District Health Information System (DHIS2), are donor-supported and often rely on external hosting.^{[11][12]} Although DHIS2 is open-source, its deployments are typically managed by international

[7] 'Africa's forgotten battleground in the US-China tech war' (Semafor News, 22 September 2025).

[8] Tanzania Communications Regulatory Authority, 'Communications Statistics Report Quarter ending September 2025' (TCRA Report, October 2025).

[9] Fabio, 'Understanding African Credit Ratings (Updated 2025)' (FurtherAfrica 12 August 2025).

[10] Ministry of ICT and National Guidance (Uganda), 'Digital Transformation Roadmap' (Report, 2023) 5.

[11] G. M. T. Mboya and others, 'Strengthening routine health data reporting in Uganda: roll-out of the District Health Management Information Software System version 2 (DHIS2)' (2014) 14(1) BMC Medical Informatics and Decision Making 45.

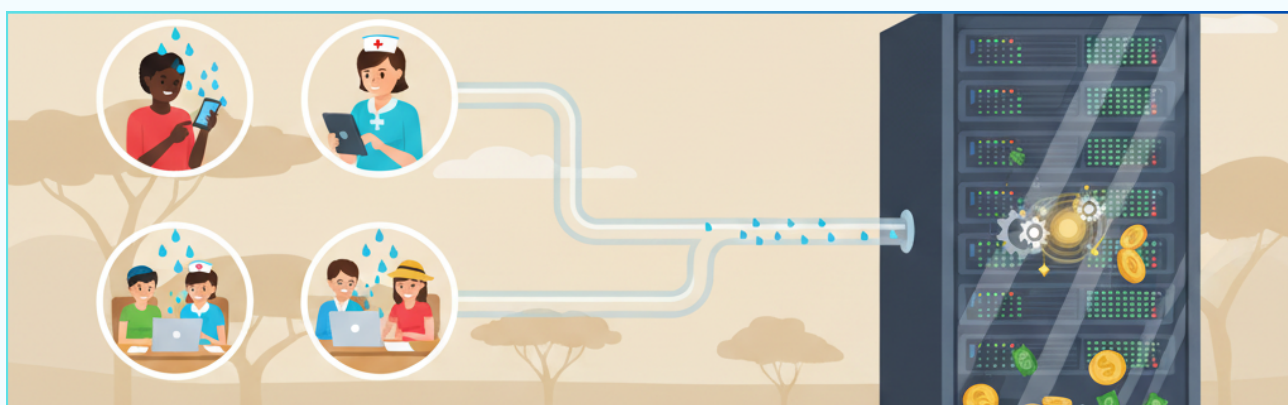
[12] 'DHIS2 for Education in Uganda' (DHIS2, 2024).

partners under terms that limit national ownership of data flows and maintenance budgets.

The data governance, hosting parameters, and long-term strategic direction of these systems are therefore intrinsically linked to donor

priorities and funding cycles, rather than a unified Ugandan national data strategy. The result is an emerging digital state whose key data assets and analytic pipelines are effectively outsourced.

3. How Data Value Is Extracted and Monetised



A Private-sector extraction through Fintech and mobile data

The mobile money revolution produced a new class of data: granular, real-time records of financial behaviour. Fintech firms such as Tala, Branch, and JUMO built entire lending models around these datasets. They combine airtime top-ups, payment patterns, and smartphone metadata to generate credit scores that enable instant microloans. While these innovations increase financial access, most of the algorithms,

data processing, and model ownership sit with foreign-incorporated companies. The value of East African behavioural data is thus captured in intellectual property and analytics revenues that accrue elsewhere. The raw data, generated locally, becomes the foundation for profitable digital financial products exported across markets.

B Public-data outsourcing through donor-funded platforms

In sectors like health and education, donors often finance digital systems to improve data collection and reporting. While these tools bring efficiency, they also create structural reliance. Hosting, software updates, and analytical dashboards are often managed by the donor or its contractors, not by national ICT agencies.

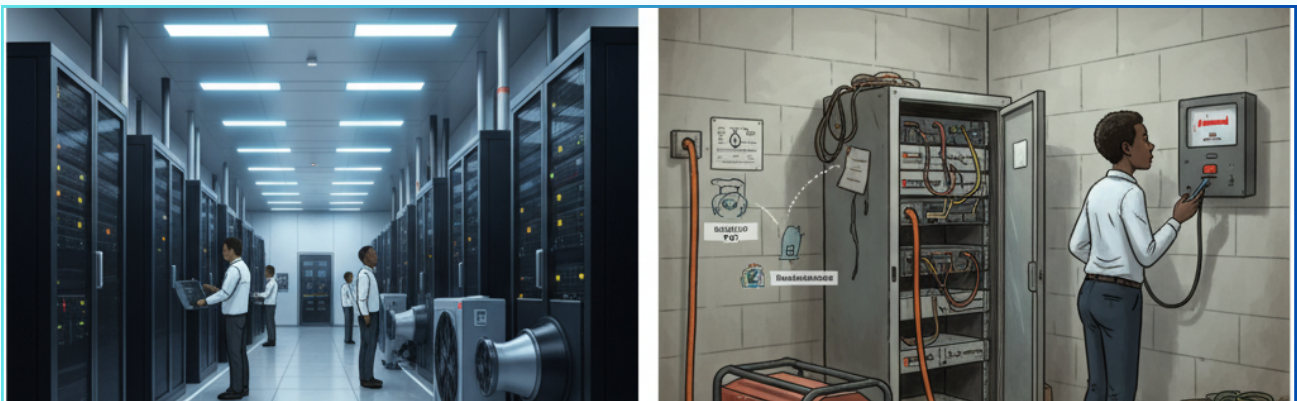
Governments gain access to reports but lack the capacity to repurpose the underlying data for broader economic or policy use. The state becomes a data client rather than a data custodian.

C Global monetisation of user data and content

East Africa's social media users generate vast amounts of content and behavioural data. This information feeds into global advertising and recommendation algorithms that shape multi-billion-dollar revenues for international technology companies. Local advertisers and media houses buy

back access to their audiences through paid campaigns. The asymmetry is striking: African data sustains global platforms, yet the local digital-advertising market captures less than two percent of the resulting value chain.

4. Why This Pattern Persists



Several structural factors account for the persistent externalisation of East Africa's data, despite increasing recognition of its significance.

High infrastructure costs and unreliable power supply

Building and operating Tier IV data centres requires significant capital and stable electricity. Local hosting is often more expensive than using global cloud services that benefit from economies of scale and advanced cooling technologies.

Donor-driven implementation logic

Donor agencies and international NGOs tend to prioritise short-term functionality over long-term sovereignty. Systems are built to deliver programme outputs, not establish national infrastructure. When funding cycles end, governments inherit maintenance costs without full control over data architecture.

Market concentration in global cloud services

Amazon, Microsoft, and Google collectively dominate more than half of the global cloud market. Their platforms offer reliability and scalability that local providers cannot yet match, making dependency almost unavoidable for start-ups and public institutions alike.

Fragmented and narrow data regulation

Existing national data protection laws focus on personal privacy, not on strategic or industrial data. They do not define ownership or jurisdiction for data generated through public-private partnerships or donor projects. Without a regional framework, external actors exploit regulatory gaps.

Skills and bargaining deficits

Negotiating fair data-sharing agreements or managing sovereign cloud infrastructure requires advanced technical and legal expertise. Many public agencies lack these capabilities, leaving them reliant on vendors to set terms and manage operations.

5. What is at stake



5.1 Economic Opportunity Cost

Data has become a production factor comparable to capital and labour. The analytics, credit models, and AI systems built from East African data could underpin local industries in finance, agriculture, and logistics.

Instead, the region imports finished digital products built on its own raw data. The forgone value manifests in missed jobs, lost taxes, and the absence of indigenous digital firms that could scale globally.

5.2 Fiscal and Industrial Implications

When foreign cloud providers and Fintechs process data abroad, their profits are booked under foreign jurisdictions, reducing taxable revenue. Local data centres development, by contrast, creates construction, energy, and ICT jobs. For example, Africa's data centre market

is projected to triple by 2030, yet most investments are still concentrated in South Africa and Nigeria, not East Africa. Without regional coordination, the EAC risks being a perpetual consumer rather than a producer of digital infrastructure.

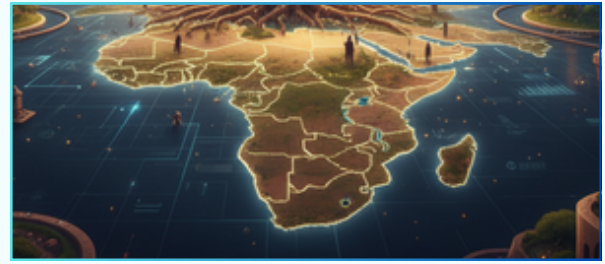
5.3 Security and Policy Risks

Dependence on foreign hosting also raises national security concerns. Data stored abroad is subject to foreign

governments spying on servers at the African Union headquarters are another example.^[13]

[13] M Bagwandeem, 'The domination of foreign companies in Africa's digital landscape could impact a country's digital sovereignty' (Global Economic Governance Programme, University of Oxford, 2023)

Moreover, when core datasets on health, agriculture, or trade are inaccessible to national analysts, governments lose the ability to make informed decisions or respond to crises effectively.

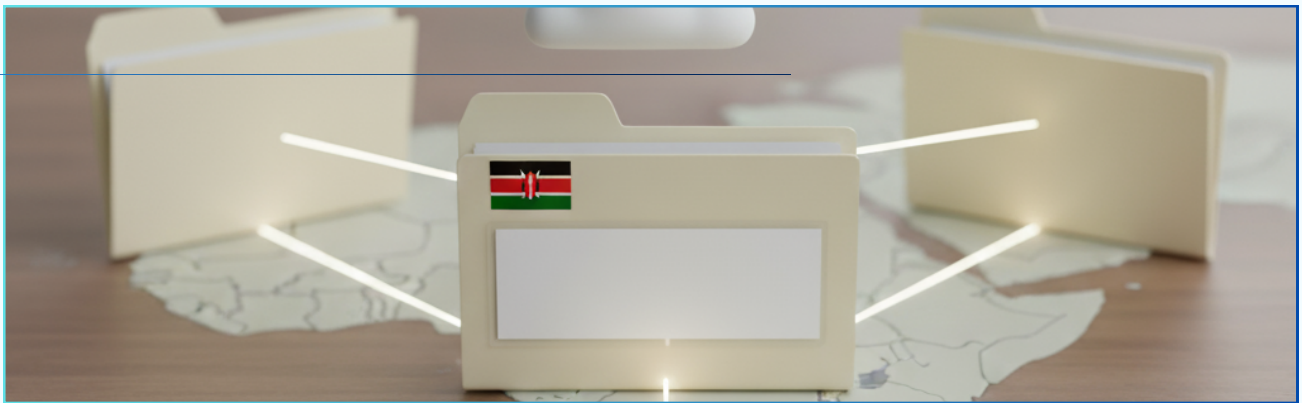


5.4 Ethical and Equity Concerns

Data about African citizens fuels AI and fintech systems that often reproduce global inequities. Credit algorithms trained on behavioural data can reinforce bias, while monetisation without benefit sharing contradicts the principles

of fairness and consent. A sovereignty framework anchored in African values of solidarity and shared benefit is therefore not only a technical necessity but also an ethical imperative.

6. Policy Landscape



Amid these challenges, cloud policy development in East Africa remains fragmented, reflecting differing national capacities and policy orientations. Kenya has made the most progress toward establishing a coherent cloud policy framework through its National Cloud Computing Policy (2023), which promotes local cloud adoption within public and

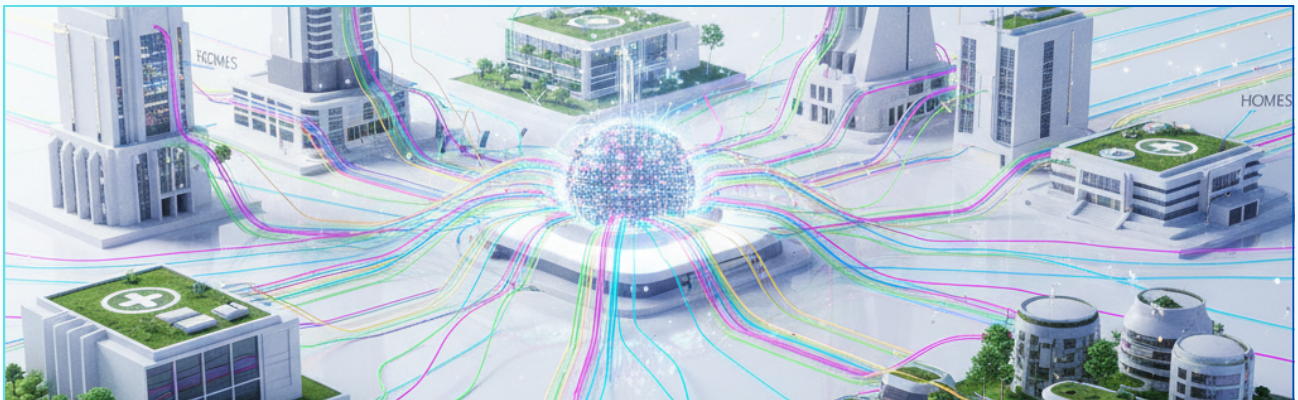
private institutions and prioritises data localisation for sensitive government information.

Innovative models for asserting data sovereignty are emerging globally. The concept of a 'data embassy', pioneered by Estonia, offers a compelling illustration of how legal

and diplomatic immunity under a bilateral treaty invoking the principles of the Vienna Convention on Diplomatic Relations.^[14] This facility serves as a secure, extraterritorial backup of Estonia's most critical government databases, ensuring the continuity of the state and the legal sovereignty of its data, even in the event of a cyber-attack or physical invasion of its territory.^[15]

The Estonian model demonstrates that sovereignty in the digital age is not solely a function of territorial control as championed by existing policies within East Africa. For the EAC, this approach presents a strategic pathway to pool resources and secure critical government data under EAC law, asserting legal jurisdiction even when physical control is delegated.

7. Opportunities for Repatriation and Innovation



● A Regional Advantage

With a combined population exceeding 330 million and growing digital adoption, the EAC has the scale to build a viable regional data economy. Pooling resources can make infrastructure investments affordable and enhance collective bargaining power with global providers.

[14] Vienna Convention on Diplomatic Relations (adopted 18 April 1961, entered into force 24 April 1964) 500 UNTS 95.

[15] S F Matinou and others, 'Beyond Borders: Exploring Data Embassies as a Strategy for Digital Sovereignty in Africa' (2024) APSA Preprints 3

● Leveraging International Law

Under the United Nations Convention on the Law of the Sea, coastal states have the authority to regulate submarine cable routing and landing. If Kenya and Tanzania coordinate under the EAC framework, they can ensure secure connectivity, transparent licensing, and equitable revenue-sharing with landlocked partners.

● Sovereign and Shared Infrastructure

A regional digital infrastructure fund could finance EAC-owned data centres powered by renewable energy. Shared facilities would reduce costs, promote interoperability, and allow governments to keep critical data within regional jurisdiction. A pilot “data embassy”, modelled on Estonia’s experience, could serve as a secure backup for vital government databases under diplomatic protection.

● Inclusive Governance as an Innovation Platform

Establishing data trusts or cooperatives would allow anonymised datasets to be shared securely with innovators and researchers while ensuring that benefits are returned to data communities. Such models could power inclusive fintech innovation, local AI development, and better public-service delivery.

8. Dependency Drivers vs. Opportunities for Sovereignty

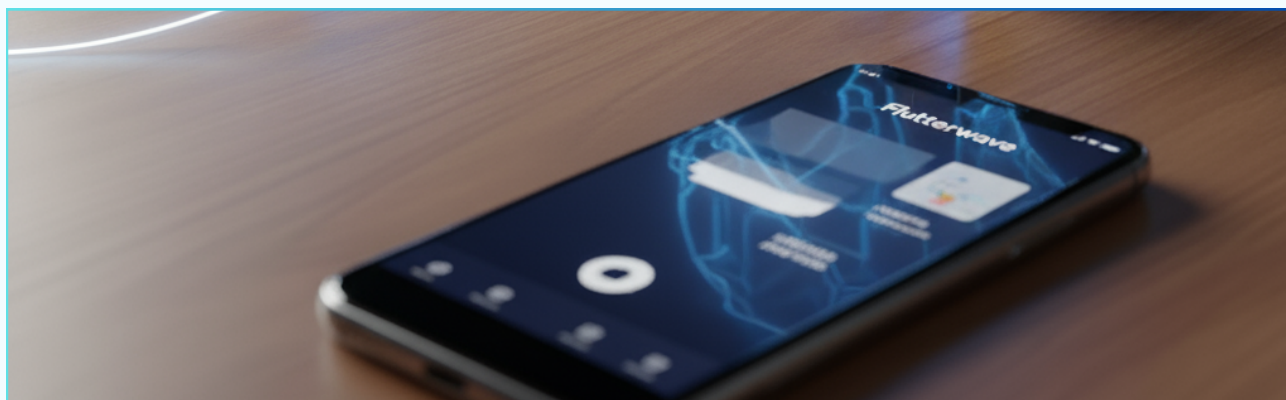
The following table summarises the core tensions between the current state of dependence and the potential for a sovereign digital future.

Table 1: Dependency drivers versus opportunities for sovereignty

Dependency Drivers (Eroding Sovereignty)	Opportunities for Sovereignty (Reclaiming Control)
Infrastructure Deficit: High cost and technical barriers to building national data centres and networks.	Shared Regional Infrastructure: Pooling resources for EAC-owned data centres, cloud platforms, and data embassies. The Government use of markets as a regulatory tool, tariff and tax breaks to bring the costs down.
Fragmented Legal Frameworks: Disparate national laws focused only on privacy, creating loopholes for external actors.	Harmonised Regional Governance: A binding EAC Data Sovereignty Framework covering all data types and asserting collective jurisdiction.
Asymmetrical Bargaining Power: Individual states negotiating with powerful Big Tech corporations and donors.	Collective Bargaining and Regulation: Jointly regulating external actors and leveraging the EAC's combined market size of 331 million people.
Donor-Tied Digital Systems: Reliance on foreign-managed platforms for critical public services (health, education).	Phased Transition to Local Control: A strategic roadmap to migrate public data to sovereign systems and build local capacity.
Underutilised International Law: Failure to collectively use existing legal instruments to govern critical infrastructure.	Strategic Invocation of UNCLOS: Jointly leveraging international law to regulate submarine cables in territorial waters.
Cultural Misalignment: Adoption of Western legal models that ignore African values of collective ownership and benefit-sharing.	African-Rooted Ethical Frameworks: Developing data trusts and cooperatives grounded in principles of solidarity and shared benefit.

Source: Author's construction

9. The Innovation Paradox – A Balanced Approach to Repatriation



While external control of data creates systemic problems, a blunt, one-size-fits-all data localisation mandate would be counterproductive, creating an ‘innovation paradox’. A credible strategy must acknowledge the significant financial, infrastructural, and human capital challenges involved. First, the initial investment in building high-quality data centres was substantial. The cost of developing a single, 1-megawatt data centre can range from USD 10 million to USD 15 million.^[16] Beyond construction, a critical issue facing data centre development in Africa is unreliable energy supply.^[17]

Second, many of East Africa’s most dynamic startups and tech firms currently depend on the affordable, scalable, and world-class cloud services provided by global giants like AWS, Microsoft Azure, and Google Cloud.^[18] Leading African Fintechs such as Flutterwave explicitly use a hybrid model: they leverage global cloud services like AWS for scalability and efficiency while using local servers to meet regulatory requirements for sensitive data.^[19]

Forcing these innovators onto nascent or more expensive local infrastructure could inadvertently increase their operational costs and reduce their competitiveness.^[20] Such policies can act as a “hidden tax on the poor” by increasing the cost of digital services for the end-users who can least afford it.^[21] The implication is clear: the EAC’s approach to data sovereignty must be strategic and sophisticated. A tiered framework for data governance is required.

10. Policy Pathways



Priority 1: Foundational Governance

- **Adopt a binding EAC Data Sovereignty Framework** that classifies data by sensitivity and defines ownership and jurisdictional rules. Working with the Council of Ministers and national Ministries of ICT and Justice, the EAC Secretariat should fast-track the finalisation and adoption of the EAC Data Governance Policy Framework as a binding regional legal instrument by the fourth quarter of 2026. This framework must go beyond the limited scope of current national data protection laws by including clear categories for non-personal, industrial, strategic, and governmental data and by introducing a tiered system of rules on jurisdiction, ownership, and cross-border transfers that safeguards security while supporting innovation.

[16] *ibid.*

[17] T Bracewell, ‘Powering Africa’s Digital Future: The Challenge of Energy for Data Center Development’ (Bracewell Resources, 2024)

[18] ‘A slice of Africa’s appetite for cloud’ (TechCabal, 26 October 2023)

[19] W McBain, ‘African tech enters the cloud’ (African Business, 22 October 2024)

[20] ‘Data Localization in Kenya and its Implication on the Digital Economy’ (ITEdge News, 2024)

[21] D Medine, ‘Data Localization: A “Tax” on the Poor’ (CGD Working Paper 674, January 2024) 1

- **Establish an EAC Data Sovereignty Council** to coordinate implementation, standard-setting, and joint negotiation with external actors. Comprising senior representatives from each partner state's national ICT authorities, the council would oversee the consistent application of the regional framework, develop technical standards, certify external data processors operating in the region, and represent the EAC in negotiations with global technology firms and international bodies. This would help address the current challenges of weak enforcement and limited independence among many national data protection authorities.

Priority 2: Strategic Infrastructure

- **Create a Regional Digital Infrastructure Fund** with contributions from member states, the African Development Bank, and private investors to build at least three Tier IV regional data centres. By 2030, this fund could use a blended finance model to attract public and private investment to co-finance carrier-neutral data centres.
- **Launch a Pilot Data Embassy Programme** by 2027, providing legal continuity for critical national datasets. Drawing inspiration from the Estonian model, the facility would operate under a regional treaty granting it diplomatic immunity, ensuring that the data of all EAC nations remains under the collective sovereign jurisdiction of the Community.

Priority 3: Assertive Regulation

- **Invoke UNCLOS provisions** to regulate submarine cables collectively, ensuring security audits and equitable access. Coastal EAC States like Kenya and Tanzania should jointly notify international maritime bodies of their collective intent to apply Article 21(c) of the United Nations Convention on the Law of the Sea (UNCLOS) through coordinated action at the EAC level.^[22] This provision grants coastal states the authority to adopt laws and regulations for the laying or routing of submarine cables within their territorial waters. The EAC should develop a common licensing framework that requires transparency on data traffic, mandatory security audits, and provisions for local partnership. A formal mechanism must be established to ensure that landlocked States are included in the governance and revenue-sharing arrangements derived from this collective assertion of sovereignty.

[22] United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 397, art 21(c).

- **Introduce a Trusted Digital Partner Certification** requiring foreign cloud providers and donors to store critical data locally, undergo regular audits, and maintain a taxable presence within the EAC. The proposed EAC Data Sovereignty Council (under priority 1) can be charged with this task. This system, inspired by federated models like Europe's GAIA-X project,^[23] balances sovereignty and innovation, allowing startups to continue using certified global services for their less sensitive commercial data.

Priority 4: Capacity and Ecosystem Development

- **Establish regional training programmes** for data governance, cybersecurity, and analytics.

- **Support data innovation hubs** that connect government, academia, and start-ups to use repatriated data for public benefit.

Implementation Roadmap

Table 1: Dependency drivers versus opportunities for sovereignty

Action	Timeline	Key Steps	Lead Actors
Adopt EAC Data Sovereignty Framework	0–18 months	Draft legal text, secure ratification	EAC Secretariat, EAC Council of Ministers, National Parliaments
Establish Data Sovereignty Council	0–18 months	Nominate representatives, define mandate	Ministries of ICT, EAC Secretariat
Jointly Invoke UNCLOS for Cable Regulation	0–18 months	Issue a joint diplomatic notification. Develop a common submarine cable licensing framework.	Ministries of Foreign Affairs and ICT, EAC Secretariat
Develop Trusted Digital Partner Certification	18–36 months	Define criteria, engage providers	EAC Data Sovereignty Council
Pilot Data Embassy Programme	18–36 months	Select host, ratify treaty, migrate data	EAC Council of Ministers, Ministries of Foreign Affairs
Establish Regional Digital Infrastructure Fund	36–60 months	Secure finance, tender data-centre projects	Finance Ministries, EAC Secretariat, AfDB

Source: Author's construction

[23] German Federal Ministry for Economic Affairs and Energy (BMWi), 'GAIA-X: The European project kicks off the next phase' (Publication, 2021) 5

11. Conclusion

East Africa's digital transformation has reached a point where progress and vulnerability coexist. The region leads in financial inclusion and mobile innovation, yet its most valuable resource, its data, remains governed and monetised elsewhere. Repatriating and governing this data collectively is not about rejecting global technology but about rewriting the terms of engagement. It is about ensuring that East African data fuels East African growth. With coordinated governance, shared infrastructure, and assertive regulation, the EAC can move from being a consumer of digital systems to being an architect of its own digital destiny.

The region now faces a simple choice: remain a data colony in the global economy, or build the foundations of a sovereign digital federation that turns data into inclusive prosperity. The time for strategic collective action is now.

Acknowledgements: *This paper was developed through the Africa's Data Future Fellowship, a CSEA initiative that builds expert capacity for evidence-based data policy in Africa. The Fellowship is part of CSEA's wider data governance programme, supported by the William and Flora Hewlett Foundation. The author gratefully acknowledges the project team's guidance and collaboration.*

Disclaimer: *The views expressed here are the author's own and do not necessarily reflect the positions of CSEA, the Fellowship, or the Hewlett Foundation. This work contributes to policy dialogue on data governance and ethical digital transformation in Africa.*