

RESEARCH TITLE

**Cloud Computing and Data Sovereignty in Developing Countries:
Challenges, Risks, and Governance Strategies**

Dr. Mohammed Ali Badawi Al-Awad Kenen¹

¹ Assistant Professor, Nile Valley University, Sudan.

HNSJ, 2026, 7(10); <https://doi.org/10.53796/hnsj710/16>

Received at 10/09/2026

Accepted at 20/09/2026

Published at 01/10/2026

Abstract

This paper examines the question of data sovereignty amid the rapid expansion of cloud computing adoption by developing countries, relying on services provided by major global technology firms. While these services deliver clear gains in cost reduction, accelerated digital transformation, and access to advanced infrastructure for smaller institutions, they simultaneously place the data of citizens, institutions, and governments in developing countries under legal and technical frameworks based outside their national borders. This raises fundamental questions about the actual degree of control such countries retain over their data and their capacity to safeguard strategic, security, and economic interests. The paper reviews the core concepts underlying cloud computing and data sovereignty, analyzes the state of digital adoption in developing countries, and discusses the principal legal, regulatory, technical, and economic challenges, alongside the security and geopolitical risks arising from excessive dependence on foreign providers. It also presents national and regional case studies in building legislative frameworks for data protection and storage regulation, concluding with a set of governance strategies and practical recommendations that policymakers in developing countries can draw upon to strike a balance between benefiting from cloud computing and preserving digital sovereignty.

Key Words: Cloud computing; Data sovereignty; Developing countries; Data governance; Digital sovereignty.

الحوسبة السحابية وسيادة البيانات في البلدان النامية: التحديات والمخاطر واستراتيجيات الحوكمة

المستخلص

تتناول هذه الورقة إشكالية سيادة البيانات في ظل التوسع المتسارع لاعتماد الدول النامية على خدمات الحوسبة السحابية المقدمة من كبريات الشركات التقنية العالمية. فبينما تتيح هذه الخدمات مكاسب واضحة في خفض التكلفة وتسريع التحول الرقمي وتمكين المؤسسات من الوصول إلى بنية تحتية متطورة، فإنها تضع في الوقت نفسه بيانات المواطنين والمؤسسات والحكومات تحت نفوذ أطر قانونية وتقنية خارج الحدود الوطنية، مما يثير تساؤلات جوهرية حول مدى السيطرة الفعلية على هذه البيانات وقدرة الدول على حماية مصالحها الاستراتيجية والأمنية والاقتصادية. تستعرض الورقة المفاهيم الأساسية للحوسبة السحابية وسيادة البيانات، وتحلل واقع التبني الرقمي في الدول النامية، وتناقش أبرز التحديات القانونية والتنظيمية والتقنية والاقتصادية، إلى جانب المخاطر الأمنية والجيوسياسية الناتجة عن الاعتماد المفرط على مزودين أجنبي. كما تعرض نماذج من التجارب الوطنية والإقليمية في وضع أطر تشريعية لحماية البيانات وتنظيم تخزينها، وتختتم بمجموعة من استراتيجيات الحوكمة والتوصيات العملية التي يمكن أن يسترشد بها صانعو السياسات في الدول النامية لتحقيق التوازن بين الاستفادة من مزايا الحوسبة السحابية والحفاظ على السيادة الرقمية.

الكلمات المفتاحية: الحوسبة السحابية؛ سيادة البيانات؛ البلدان النامية؛ حوكمة البيانات؛ السيادة الرقمية.

Executive Summary

This paper examines the question of data sovereignty amid the rapid expansion of cloud computing adoption by developing countries, relying on services provided by major global technology firms. While these services deliver clear gains in cost reduction, accelerated digital transformation, and access to advanced infrastructure for smaller institutions, they simultaneously place the data of citizens, institutions, and governments in developing countries under legal and technical frameworks based outside their national borders. This raises fundamental questions about the actual degree of control such countries retain over their data and their capacity to safeguard strategic, security, and economic interests.

The paper reviews the core concepts underlying cloud computing and data sovereignty, analyzes the state of digital adoption in developing countries, and discusses the principal legal, regulatory, technical, and economic challenges, alongside the security and geopolitical risks arising from excessive dependence on foreign providers. It also presents national and regional case studies in building legislative frameworks for data protection and storage regulation, concluding with a set of governance strategies and practical recommendations that policymakers in developing countries can draw upon to strike a balance between benefiting from cloud computing and preserving digital sovereignty.

Introduction

The world is undergoing a fundamental shift in how data is stored, processed, and managed. Government and private institutions no longer rely primarily on locally owned data centers; instead, they are increasingly turning to cloud computing, which offers high flexibility, lower costs, and immense on-demand computing power. These characteristics have made cloud computing a particularly attractive option for developing countries, which often lack the financial and technical resources needed to build integrated national digital infrastructure.

Yet this transition is not without profound complications, chief among them the issue of data sovereignty — the state's right to apply its laws and controls over data related to its citizens and institutions regardless of where that data is physically stored. Most major cloud service providers are headquartered in the United States, China, or Europe, and are therefore subject to the legislation of those countries, which may grant them authority to access data stored on their servers even when it concerns citizens or institutions of other nations. This creates a potential conflict between the legal sovereignty of the country hosting the data and that of the country to which the service provider belongs.

This issue carries particular weight for developing countries for several reasons: weak national legislative frameworks for data protection, limited bargaining power vis-à-vis technology giants, the absence of viable local cloud infrastructure alternatives, and the political and security sensitivity of certain categories of data such as national identity records, health data, financial data, and sensitive government information. This paper aims to provide a comprehensive analysis of these issues, culminating in practical, actionable recommendations.

Objectives of the Paper

1. Clarify the core concepts of cloud computing and data sovereignty and their legal and technical dimensions.
2. Analyze the state of cloud computing adoption in developing countries and its driving factors.
3. Review the principal legal, regulatory, and technical challenges facing these countries.

4. Identify the security, economic, and geopolitical risks arising from dependence on foreign providers.
5. Present comparative examples from the experiences of developing and emerging economies in regulating this field.
6. Propose governance strategies and practical recommendations for policymakers.

Core Concepts

The Concept of Cloud Computing

Cloud computing is defined as a model for delivering computing resources — such as servers, storage, databases, networking, and software — over the internet on a pay-as-you-go basis, rather than owning and maintaining physical infrastructure locally. Cloud services are typically divided into three main models:

- Infrastructure as a Service (IaaS): provision of basic computing resources such as virtual servers and storage units.
- Platform as a Service (PaaS): an integrated environment for developing and deploying applications without managing underlying infrastructure.
- Software as a Service (SaaS): ready-made applications accessed by users over the internet without local installation.

Clouds are also classified by ownership and access into public clouds managed by a commercial company and available to the general public, private clouds dedicated to a single entity, hybrid clouds combining both models, and community clouds shared among several entities with common interests, such as the public sector.

The Concept of Data Sovereignty

Data sovereignty refers to the principle that digital data is subject to the laws and regulatory frameworks of the country in which it was collected or to which its owners belong, regardless of where it is physically stored. This concept is closely related to three neighboring notions worth distinguishing:

- Data Residency: the requirement that data be physically stored within specific geographic boundaries, without necessarily restricting who may legally access it.
- Data Localization: legal requirements obligating companies to process and store certain categories of data locally, sometimes prohibiting cross-border transfer except under specific conditions.
- Data Sovereignty: a broader concept encompassing a state's right to full legal and regulatory control over data related to its citizens, including who may access, process, and transfer it — even when stored abroad.

This issue is compounded by so-called extraterritorial laws, the most prominent example being the U.S. CLOUD Act of 2018, which grants American authorities the power to compel U.S. technology companies — such as Microsoft, Amazon, and Google — to hand over data stored on their servers anywhere in the world. This places countries that rely on these companies for data storage in a complex legal position, as they may effectively become subject to foreign legal sovereignty without their explicit knowledge or consent.

The Relationship Between the Two Concepts: Intersection and Tension

The complex relationship between cloud computing and data sovereignty arises from the very nature of cloud infrastructure, which is built on distributing data across multiple data centers

worldwide for efficiency, availability, and service continuity. When a developing country relies on a global cloud provider, it typically lacks full control over the actual physical location of its data, over the laws governing third-party access to it, and even over its ability to fully retrieve its data should it decide to switch providers — a problem known as vendor lock-in.

The State of Cloud Computing Adoption in Developing Countries

Developing countries are experiencing accelerated growth in cloud service adoption, driven by a set of interlocking economic, technical, and social factors. On one hand, these services offer a cost-effective alternative to investing in expensive local infrastructure; on the other, they help accelerate government digital transformation initiatives and enable startups to compete without the need for massive capital.

Drivers of Adoption

- Reduced capital expenditure: shifting spending from capital outlays (building data centers) to flexible, usage-based operational expenses.
- Speed of deployment and scaling: the ability to launch new government or commercial digital services within weeks rather than years.
- Access to advanced technologies: leveraging artificial intelligence and big-data analytics capabilities that would be difficult to develop locally.
- Support for government digital transformation programs: e-government initiatives increasingly rely on cloud platforms to deliver public services.
- The COVID-19 pandemic, which accelerated the shift toward remote work, digital education, and e-commerce.

Limited Local Infrastructure

Most developing countries suffer from clear weaknesses in the digital infrastructure required to host large volumes of data locally — whether measured by the number of internationally certified data centers, the reliability of electricity supply, or the capacity of connections to international internet backbones via submarine cables. This reality makes dependence on foreign cloud providers a near-obligatory choice in the short and medium term, even for countries that recognize the sensitivity of their national data.

Dominance of a Limited Number of Providers

The global cloud computing market is dominated by a small number of major companies, most notably Amazon Web Services, Microsoft Azure, and Google Cloud, alongside Chinese providers such as Alibaba Cloud and Huawei Cloud, whose presence is growing rapidly in Africa and Asia. This dominance leads to an imbalanced concentration of control over the data of billions of users worldwide in the hands of a few entities subject to a limited number of legal jurisdictions — deepening the data sovereignty dilemma for countries lacking a competitive national or regional alternative.

Legal and Regulatory Challenges

Weak or Absent National Data Protection Legislation

Dozens of developing countries still lack comprehensive personal data protection laws, or rely on fragmented provisions scattered across telecommunications or e-commerce laws that fail to adequately address issues such as cross-border transfers, individual data rights, or the obligations of cloud service providers. This legislative vacuum leaves broad room for divergent interpretations and inconsistent practices by companies operating in these markets.

Conflicting Jurisdictions

The inherently cross-border nature of cloud computing creates potential conflicts among several legal frameworks: the law of the country where the data was collected, the law of the country where the data center is physically located, and the law of the country where the service provider's headquarters is based. This overlap may leave a developing country practically unable to enforce its domestic laws over its citizens' data if a foreign judicial authority requests it under legislation such as the U.S. CLOUD Act or similar statutes.

Unequal Service Contracts

Standard cloud computing contracts offered by major companies are typically uniform contracts of adhesion, leaving little room for negotiation by customers in developing countries, whether governments or small enterprises. These contracts usually include clauses concerning liability limits, governing law, jurisdiction for disputes, and terms for service termination and data retrieval — provisions that may disadvantage developing-country clients who lack the specialized legal expertise and negotiating leverage needed to amend them.

Absence of Independent, Effective Regulatory Bodies

Even in countries that have enacted data protection legislation, newly established data protection authorities often suffer from insufficient financial, human, and technical resources needed to exercise their oversight role effectively — whether in monitoring corporate compliance, investigating complaints, or imposing penalties for violations — leaving legal frameworks more theoretical than practically enforced.

Security, Economic, and Geopolitical Risks

Security Risks

- Exposure of sensitive data (such as government, military, and health data) to unauthorized access by foreign entities under the domestic legislation of the provider's home country.
- Increased cyberattack surface resulting from reliance on shared infrastructure managed by a third party outside the state's direct oversight.
- Risk of service disruption or loss of data access in the event of a commercial or political dispute with the service provider or its home country.
- Difficulty conducting independent, comprehensive security audits on infrastructure owned by an external party.

Economic Risks

- Outflow of hard currency abroad in the form of subscription fees for cloud services, rather than investment in building local capacity.
- The vendor lock-in problem and the high cost of switching between service providers, weakening the customer's future negotiating position.

- Hindered growth of the local IT sector and national data center industry due to unequal competition with global giants.
- Limited local value addition, as high-skill functions (such as algorithm and infrastructure development) remain concentrated at parent company headquarters.

Geopolitical and Political Risks

- Deepening digital dependency on major technology powers (primarily the United States and China), limiting the strategic autonomy of developing countries.
- The potential use of data as a tool of political or economic pressure in international disputes or sanctions.
- Risks related to mass surveillance or the use of data for intelligence purposes by foreign states.
- Challenges related to technological neutrality, as some countries may find themselves forced to choose between competing technology ecosystems (American or Chinese), carrying political implications.

Comparative Table: Key Risks by Nature and Impact Level

Risk Type	Description	Impact Level
Security	Unauthorized access to sensitive data via foreign legislation or cyberattacks	High
Economic	Hard-currency outflow, weak local industry, and vendor lock-in	Medium to High
Legal	Conflicting jurisdictions and weak enforcement of domestic law	High
Geopolitical	Deepening digital dependency and potential use of data as leverage	Medium to High
Operational	Service disruption or loss of access during commercial or technical disputes	Medium

National and Regional Case Studies

A number of developing and emerging economies have developed legislative and institutional frameworks to address the data sovereignty dilemma, though their maturity and practical effectiveness vary. The most notable examples include:

Nigeria

Nigeria issued the Nigeria Data Protection Regulation (NDPR) in 2019, which mandates specific data handling practices and imposes restrictions on transferring certain data abroad absent adequate safeguards. This framework was later reinforced by the establishment of the Nigeria Data Protection Commission as an independent regulatory body, marking a step toward institutionalized data protection oversight.

Kenya

Kenya enacted its Data Protection Act in 2019, largely inspired by the European Union's General Data Protection Regulation (GDPR), which includes specific provisions on cross-border data transfers, requiring either an equivalent level of protection in the receiving country or the presence of appropriate contractual safeguards.

Rwanda

Rwanda stands out among African nations for its ambitious approach, having enacted its Law on Data Protection and Privacy in 2021 while simultaneously investing in national cloud infrastructure and internationally certified data centers as part of its strategy to become a regional information technology hub.

India

India has adopted a relatively strict localization approach in specific sectors, most notably the Reserve Bank of India's requirement that payment companies store transaction data exclusively within India, within the framework of a broader legislative debate that culminated in the Digital Personal Data Protection Act enacted in 2023.

The African Union: The Malabo Convention

The African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, in 2014, aiming to establish a unified continental framework for data protection. However, its actual entry into force was delayed for years due to slow ratification by member states, reflecting the institutional challenge of achieving effective regional coordination.

China and Russia: The Strict Localization Model

China and Russia represent an alternative model based on imposing strict restrictions on the storage and transfer of certain data. China's Cybersecurity Law and Personal Information Protection Law require that certain data be stored locally and undergo security review before any cross-border transfer, while Russian law since 2015 has required that the personal data of Russian citizens be stored within Russian territory. While this model strengthens national control, it faces criticism related to restricting the free flow of information and its occasional use as a tool of surveillance.

Proposed Governance Strategies

The data sovereignty dilemma cannot be addressed through a single measure or isolated decision; it requires a multidimensional approach combining legislative, institutional, technical, and diplomatic dimensions. The following are the principal pillars of a proposed governance strategy:

Legislative and Regulatory Pillar

- Enact comprehensive personal data protection legislation that clearly defines sensitive data categories and the requirements for their transfer and processing.
- Classify data by sensitivity level (public data, ordinary personal data, sensitive data, strategic national-security data) and apply graduated storage and processing requirements proportionate to each category, rather than imposing blanket, impractical localization.
- Require the inclusion of standard contractual clauses in cloud service agreements that clearly specify the applicable jurisdiction, dispute resolution mechanisms, and data retrieval guarantees.
- Establish an independent national data protection authority with genuine oversight and enforcement powers and adequate resources.

Institutional and Capacity-Building Pillar

- Invest in training national personnel in cybersecurity, digital law, and technical contract management.

- Establish national or regional centers of excellence on data governance to provide technical support to government bodies in evaluating cloud computing contracts.
- Strengthen coordination among relevant government bodies (telecommunications regulation, data protection, cybersecurity, trade) to avoid conflicting policies.

Technical and Infrastructure Pillar

- Encourage investment in national or regional data centers, whether through public-private partnerships or by pooling regional demand to achieve economic viability.
- Adopt sovereign cloud models for highly sensitive data — a cloud infrastructure managed by national entities or governed by special contracts ensuring that data and control over it remain within the national jurisdiction.
- Adopt data portability and interoperability standards to avoid single-vendor lock-in and facilitate switching between providers when needed.
- Promote multi-cloud strategies to reduce the risk of concentration with a single provider.

Regional and Diplomatic Pillar

- Strengthen regional integration in developing unified data protection frameworks, similar to efforts under the African Malabo Convention or comparable initiatives in Southeast Asia and Latin America, to enhance collective bargaining power vis-à-vis major companies.
- Pursue bilateral or multilateral negotiations on adequacy agreements to regulate data flows with key trading partners.
- Participate actively in international forums on internet and data governance to ensure developing countries' interests are represented in the formulation of global standards.

A Balanced Approach: Avoiding Excessive Localization

It is worth noting that excessive, blanket localization requirements for all data types may backfire, raising the cost of digital services, limiting the ability of local startups to benefit from global cloud advantages, and potentially excluding the country from access to advanced technological innovations. Most specialized studies therefore recommend a gradual, proportionate approach that concentrates strict localization on the most sensitive data categories only, while adopting more flexible contractual and technical controls for other data types.

Recommendations

7. Establish a clear national data classification system based on sensitivity level, to inform storage, processing, and cross-border transfer requirements for each category.
8. Enact or update personal data protection legislation to keep pace with technological developments while safeguarding individual rights and provider obligations.
9. Establish independent regulatory bodies with adequate resources to oversee compliance and impose penalties for violations.
10. Develop standardized contract templates for cloud provider agreements that safeguard the state's right to retrieve its data and clearly define applicable jurisdiction.
11. Invest progressively in national or regional cloud infrastructure, beginning with the most sensitive government data.

12. Adopt a hybrid, multi-provider cloud model to reduce the risk of single-vendor lock-in.
13. Strengthen regional cooperation to harmonize regulatory standards and increase collective bargaining power vis-à-vis global companies.
14. Build national capacity in cybersecurity and digital law through continuous training programs for government and technical personnel.
15. Conduct periodic risk assessments of existing cloud computing contracts, with contingency plans for switching providers when necessary.
16. Encourage transparency from service providers regarding data storage locations and policies on responding to requests from foreign government authorities.

Conclusion

Cloud computing represents an indispensable tool for accelerating digital transformation in developing countries, offering economic efficiency and advanced technical capabilities that would be difficult to achieve with local resources alone. However, these benefits should not obscure the genuine legal, security, economic, and geopolitical risks posed by the data sovereignty dilemma — particularly given the dominance of a limited number of global companies subject to extraterritorial legislation.

The balance required does not lie in digital isolation through blanket, impractical localization, nor in unrestricted openness that exposes national sovereignty to risk, but rather in adopting a gradual, proportionate approach that combines sound legislation, institutional and technical capacity-building, progressive investment in national and regional infrastructure, and effective diplomatic coordination. In this way, developing countries can reap the benefits of the cloud revolution without sacrificing their digital sovereignty or long-term strategic interests.

References

- United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report, various years.
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014.
- U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018.
- Nigeria Data Protection Regulation (NDPR), 2019; Nigeria Data Protection Act, 2023.
- Kenya Data Protection Act, 2019.
- Rwanda Law on Data Protection and Privacy, 2021.
- Reserve Bank of India, Directive on Storage of Payment System Data, 2018; India Digital Personal Data Protection Act, 2023.
- OECD, Going Digital: Shaping Policies, Improving Lives, and related reports on data governance.
- World Bank, World Development Report: Data for Better Lives, 2021.
- European Union, General Data Protection Regulation (GDPR), 2016.