

The GLOCEPS

Policy Brief

Strengthening Kenya's Digital Sovereignty for National Resilience and Economic Competitiveness

Anita Onuko, Stephen Nduvi, Denis Muniu & Mike Owuor

Executive Summary

Kenya has emerged as one of Africa's leading digital economies through sustained investments in digital public infrastructure, mobile financial services, innovation ecosystems, and electronic government services. Flagship initiatives, including the Digital Superhighway Programme, Konza Technopolis, and the National Artificial Intelligence Strategy 2025 to 2030, have accelerated digital transformation and strengthened Kenya's position as a regional technology hub. However, increasing dependence on foreign owned digital infrastructure and external data ecosystems presents strategic risks to national resilience, economic competitiveness, and policy autonomy.

This brief argues that strengthening digital sovereignty, defined as the state's capacity to independently govern, secure, and derive economic value from its critical digital assets while maintaining beneficial global technology partnerships, is essential for securing Kenya's digital future. It identifies four interconnected policy challenges. First, an estimated 95 percent of government data resides on foreign owned cloud infrastructure, exposing critical systems to cyber risks, supply chain disruptions, and external jurisdiction. Second, artificial intelligence, digital platforms, and cyber threats are outpacing existing governance frameworks, creating regulatory gaps. Third, research and development investment remains at 0.4 percent of GDP, while limited artificial intelligence

talent constrains technology production. Fourth, digital diplomacy and regional digital leadership remain underutilized.

To address these challenges, Kenya should adopt a National Digital Sovereignty Strategy integrating digital infrastructure, data governance, artificial intelligence, cybersecurity, innovation policy, and international cooperation. Strengthening trusted digital systems, investing in indigenous digital capabilities, and advancing regional digital governance will enhance resilience, increase economic value creation, and consolidate Kenya's position as a leading digital economy in Africa.



Photo Credit: Chu4uhc.Org



Context

Digital technologies are fundamentally reshaping global economic systems, governance structures, national security frameworks, and international relations. Artificial intelligence, cloud computing, big data, digital platforms, and digital public infrastructure have evolved from commercial tools into strategic assets that determine countries' economic competitiveness, innovation capacity, and geopolitical influence. As digital technologies become embedded within critical sectors such as finance, healthcare, education, energy, transport, and public administration, governments are increasingly focusing not only on expanding digital access but also on strengthening their capacity to govern, secure, and derive value from digital ecosystems.

Globally, countries are adopting digital sovereignty strategies aimed at reducing strategic vulnerabilities while maintaining participation in interconnected global markets. The European Union's Gaia-X initiative, India's India Stack and data localization requirements, and Nigeria's revised National Digital Economy Policy and Strategy (2020-2030) exemplify approaches that seek to exercise strategic choice over critical digital infrastructure, enhance data governance, promote responsible artificial intelligence development, protect cybersecurity resilience, and support indigenous technological capabilities. Digital sovereignty does not imply technological isolation or rejection of international partnerships; rather, it reflects a country's ability to exercise strategic choice, regulate critical digital assets, and participate in the global digital economy from a position of greater capability and resilience.

Kenya has made significant progress in digital transformation and has established itself as one of

Africa's leading digital economies. The success of mobile financial services, particularly M-Pesa which now processes over KSh 35 trillion annually, expanding broadband connectivity through the 10,000-kilometer National Optic Fibre Backbone Infrastructure, growth of technology enterprises, and establishment of the Konza Technopolis as a dedicated innovation district demonstrate the country's commitment to leveraging technology for economic transformation. These initiatives support national development priorities by enhancing service delivery, promoting innovation, expanding digital inclusion, and strengthening Kenya's competitiveness within the regional and global digital economy.

Despite these achievements, Kenya's digital ecosystem remains characterized by significant dependence on foreign-owned cloud infrastructure including Amazon Web Services, Microsoft Azure, and Google Cloud, multinational digital platforms, externally developed artificial intelligence systems, and cross-border data processing arrangements. While these partnerships have accelerated technological advancement, they also create strategic vulnerabilities related to cybersecurity, data governance, supply chain disruptions, the extra-territorial reach of foreign legislation such as the United States CLOUD Act, and limited domestic value creation. The increasing importance of artificial intelligence and data-driven innovation further underscores the need for Kenya to strengthen control over strategic digital resources while fostering global cooperation. The primary policy challenge is therefore not whether Kenya should participate in the global digital economy, but how it can strengthen domestic capabilities while maintaining beneficial international technology partnerships.



At the same time, emerging continental frameworks, including the African Union Digital Transformation Strategy 2020–2030, the African Continental Free Trade Area Digital Trade Protocol, the Malabo Convention on Cyber Security and Personal Data Protection, the Smart Africa Alliance, and East African Community digital integration initiatives, provide opportunities for Kenya to shape regional approaches to digital governance. By strengthening domestic capabilities while advancing collective African digital interests, Kenya can enhance technological resilience, promote inclusive innovation, and consolidate its position as a strategic leader in Africa's digital transformation.

The rapid evolution of artificial intelligence, digital platforms, and cyber threats further increases the complexity of digital governance. The National Artificial Intelligence Strategy 2025–2030, the Data Protection (General) Regulations 2021, and the National Cybersecurity Strategy 2022–2027 provide important foundations. However, these instruments require continuous adaptation to address emerging challenges such as algorithmic bias, AI-generated misinformation, cyber-enabled economic crime, digital influence operations, and vulnerabilities affecting critical information infrastructure across the finance, energy, health, and telecommunications sectors. Without coordinated governance approaches, technological advancement may deepen existing inequalities, undermine public trust, and expose critical systems to emerging security threats.

Furthermore, Kenya's transition from a technology adoption model towards technology production remains constrained by limited investment in

research and development, with public R&D expenditure concentrated in agriculture and health while digital technologies receive less than 12% of total research funding, shortages of advanced digital skills, venture capital availability below KSh 10 billion annually for deep-tech startups, and weak commercialization pathways for indigenous innovations. Without stronger domestic capabilities, Kenya risks remaining primarily a consumer of externally developed technologies rather than becoming a producer of digital solutions capable of competing regionally and globally.

Addressing these risks requires a comprehensive digital sovereignty framework that integrates infrastructure development, data governance, artificial intelligence regulation, cybersecurity resilience, digital industrial policy, skills development, and international cooperation. A coordinated national approach will enable Kenya to reduce strategic vulnerabilities while preserving openness to global innovation, investment, and technological partnerships.



Key Issues

The following issues remain pertinent in strengthening Kenya's digital sovereignty.

Dependence on Foreign Digital Infrastructure and Data Ecosystems

Kenya's digital transformation has generated significant economic and governance benefits. However, growing dependence on externally controlled digital infrastructure, data ecosystems, and artificial intelligence capabilities presents a strategic vulnerability. The National Transport and Safety Authority, the Judiciary e-filing system, and multiple county government databases operate on foreign cloud services governed by non-Kenyan law. While international technology partnerships have accelerated digital development, excessive reliance on foreign-owned cloud services, digital platforms, and AI systems may constrain Kenya's ability to secure critical digital assets, influence technology standards, and capture greater economic value from its digital economy. The 2023 global outage of a major cloud provider that disrupted Kenyan financial services illustrates the operational risks of this dependency.

Data sovereignty represents a related challenge. As data increasingly drives artificial intelligence, innovation, research, and digital trade, countries with stronger data governance capabilities are better positioned to generate economic value and shape technological development. Although Kenya has established a robust data protection framework under the Office of the Data Protection Commissioner established in 2020, fragmented data-sharing systems and significant external processing of Kenyan data constrain opportunities for local innovation and strategic oversight. The

absence of a national data registry identifying where government data is stored and processed prevents systematic risk assessment.

Artificial intelligence introduces additional dependency risks due to Kenya's reliance on foreign-developed models, computing infrastructure, and datasets. Kenyan businesses and government agencies predominantly use AI systems developed by OpenAI, Google, Meta, and Microsoft, trained on non-Kenyan data and optimized for non-African contexts. This reliance on externally developed AI systems creates challenges relating to algorithmic transparency, accountability, bias, and alignment with Kenya's socio-economic realities. The limited availability of locally relevant datasets, insufficient AI research capacity, and gaps in technical expertise may reduce Kenya's ability to develop, evaluate, and govern AI systems effectively. Without investment and appropriate safeguards in local AI research capacity, high-quality datasets, and advanced computing capabilities, Kenya risks remaining a technology consumer rather than a producer of AI solutions suited to African contexts.

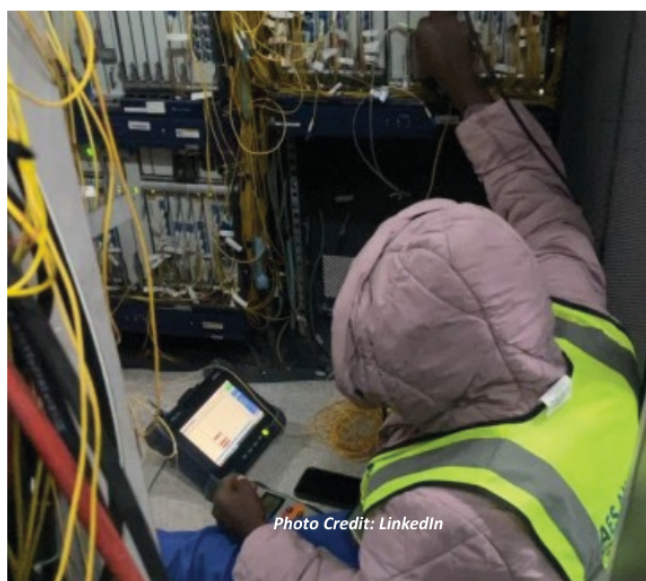


Photo Credit: LinkedIn



Addressing these challenges requires a strategic approach that strengthens domestic capabilities without pursuing technological isolation. Establishing a Government Sovereign Cloud certified to Tier III standards or higher, mandating data classification and residency requirements for sensitive public data, and funding the development of open-source Swahili and local language AI models will enhance national resilience, promote technological competitiveness, and enable Kenya to derive greater economic value from the digital economy.

Domestic Digital Capabilities and Technological Competitiveness

Kenya's long-term digital sovereignty will depend not only on regulating digital technologies but also on its ability to develop, produce, and competitively deploy indigenous technological solutions. While the country has established itself as a leading African digital innovation hub through mobile financial services, technology entrepreneurship, and digital public infrastructure, sustaining this position requires a transition from technology adoption towards technology production, research, and digital industrialization.

Kenya's current digital ecosystem demonstrates strong entrepreneurial capacity evidenced by Nairobi's consistent ranking among Africa's top three startup ecosystems but remains constrained by limited investment in research and development, insufficient financing for frontier technologies, shortages of advanced technical skills, and weak pathways for commercializing locally developed innovations. These constraints limit the ability of Kenyan enterprises, universities, and research institutions to participate meaningfully in high-value digital value chains, particularly in areas such as artificial intelligence, cloud computing, cybersecurity,

advanced software development, and emerging technologies. Kenyan firms currently capture less than 15% of the value in government IT procurement, with the remainder flowing to multinational vendors and system integrators.



Photo Credit: World Bank

The absence of strong domestic technological capabilities creates strategic vulnerabilities because countries that depend primarily on imported technologies have limited influence over the design, adaptation, and governance of digital systems. Building digital sovereignty therefore requires strengthening the capacity of Kenyan institutions and enterprises to develop solutions that respond to local challenges, support economic transformation, and compete in regional and global markets. This includes committing to increase Gross Expenditure on R&D from the current estimated 0.4% to at least 1% of GDP by 2030, establishing a dedicated high-performance computing facility accessible to researchers and startups, and implementing the long-pending Technology Transfer Bill to facilitate commercialization of publicly funded research.



Digital capabilities are also central to Kenya's industrial transformation agenda. Technologies such as artificial intelligence, data analytics, digital manufacturing, and automation can enhance productivity across agriculture, manufacturing, healthcare, logistics, and public services. However, these benefits will only be realized if Kenya develops the skills base, institutional partnerships, and innovation ecosystems required to translate technological potential into economic value. Kenya should therefore adopt a coordinated digital industrial policy that aligns technology development with the Bottom-Up Economic Transformation Agenda's priority value chains in agriculture, housing, healthcare, and the digital economy.

Governance of Emerging Digital Technologies, Digital Platforms and Cyber Resilience

The rapid adoption of artificial intelligence, digital platforms, and interconnected digital systems is creating new governance challenges that extend beyond technological innovation. While these technologies provide significant opportunities to improve public service delivery, enhance productivity, strengthen financial inclusion, and accelerate economic transformation, inadequate governance frameworks may expose Kenya to emerging risks affecting national security, democratic resilience, and public trust.

Digital platforms have also become powerful actors shaping information ecosystems, economic transactions, and public discourse. Social media platforms, search engines, and digital marketplaces increasingly influence how information is created, distributed, and consumed. However, decisions relating to content moderation, algorithmic visibility, political advertising, and user access are often

governed by multinational companies operating outside Kenya's regulatory environment. During Kenya's 2022 general election, foreign-owned platforms made critical content moderation decisions affecting political speech without transparent criteria or domestic accountability mechanisms. The growth of misinformation, disinformation, AI-generated synthetic content, and cyber-enabled influence operations presents additional risks to democratic processes, social cohesion, and institutional trust.



At the same time, cybersecurity has become a critical component of national resilience as government systems, financial infrastructure, telecommunications networks, and essential services become increasingly digitized. The Communications Authority of Kenya reported a 300% increase in cyber threats between 2020 and 2023, with ransomware attacks targeting SMEs, financial institutions, and county governments. The growing sophistication of ransomware, artificial intelligence-enabled cyberattacks, phishing campaigns, and supply chain compromises requires a more proactive and coordinated cybersecurity approach.



Kenya has taken important steps to strengthen digital governance through the National Artificial Intelligence Strategy, the Data Protection Act, the Computer Misuse and Cybercrimes Act, and the establishment of the National Computer and Cybercrimes Coordination Committee and the Office of the Data Protection Commissioner.

The recent release of the Draft Kenya Artificial Intelligence and Other Emerging Technologies Policy for public participation on 21 July 2026 further reinforces this trajectory by providing the governance, ethical, regulatory, and institutional framework necessary to guide implementation of the National AI Strategy. Together, the Strategy and the draft Policy strengthen Kenya's AI ecosystem by ensuring that technological innovation and adoption are underpinned by responsible governance, public trust, regulatory certainty, and long-term digital resilience.

Nevertheless, technological innovation continues to outpace regulatory adaptation. Artificial intelligence applications, algorithmic decision-making, digital platforms, and cyber threats are evolving faster than existing governance frameworks, creating regulatory gaps that could undermine economic resilience, democratic governance, and public confidence in digital systems. The increasing use of generative artificial intelligence further heightens the risks of misinformation, identity fraud, election interference, and sophisticated cyber-attacks.

Digital Diplomacy and Africa's Collective Digital Sovereignty

Kenya should therefore strengthen integrated governance of emerging technologies by developing

adaptive regulatory frameworks that establish a statutory duty on platform operators to conduct and publish algorithmic risk assessments, create a mandatory incident notification regime for AI-related harms, and empower sector regulators to issue binding technical standards for AI deployment in high-risk domains including finance, health, and law enforcement. A trusted digital ecosystem will enable Kenya to harness technological innovation while safeguarding national security, democratic resilience, and public confidence.

International cooperation, global technology standards, and geopolitical competition over emerging technologies will increasingly shape the future of digital sovereignty. Issues such as artificial intelligence governance, cross-border data flows, cybersecurity, digital trade, digital taxation, and technology supply chains are becoming central components of international relations. For Kenya, advancing digital sovereignty therefore requires not only strengthening domestic capabilities but also actively shaping regional and global digital governance frameworks.



Photo Credit: SAIIA



Kenya's successful representation of African interests in the Global Digital Compact negotiations and its leadership within the Smart Africa Alliance demonstrate the potential of proactive digital diplomacy. However, many digital governance challenges transcend national borders. Cyber threats, data flows, digital trade, technology standards, and platform regulation require coordinated approaches that individual countries may struggle to address independently.

Regional and continental frameworks, including the African Union Digital Transformation Strategy 2020–2030, the African Continental Free Trade Area Digital Trade Protocol, the Smart Africa Alliance, and East African Community digital integration initiatives, provide opportunities for collective action. Through these platforms, African countries can harmonize digital regulations, strengthen cybersecurity cooperation, promote trusted cross-border data flows, and develop common positions in negotiations with global technology companies. Greater coordination would also enhance Africa's influence in international discussions on artificial intelligence governance, digital standards, and responsible technology development. The African Union's forthcoming AI Continental Strategy and the ongoing negotiation of a global digital compact offer immediate opportunities for Kenya to exercise leadership.

For Kenya, digital diplomacy should become an integral component of foreign policy and economic strategy. The country can leverage its technological strengths to promote regional digital integration, attract responsible technology investment, support

African participation in global technology governance forums, and advance inclusive digital development. This requires the establishment of a dedicated Digital Diplomacy Directorate within the Ministry of Foreign and Diaspora Affairs, appointment of specialized technology attachés in key diplomatic missions including Brussels, Geneva, and Washington D.C., and regular coordination between the Ministry and the Ministry of Information, Communications and the Digital Economy on international technology negotiations.

Kenya should therefore position digital diplomacy as a strategic instrument for strengthening both national and continental digital sovereignty. By combining domestic technological capabilities with regional cooperation, Kenya can enhance its bargaining power, shape global digital norms, and contribute to the development of a secure, inclusive, and competitive African digital ecosystem.



Conclusion

Kenya's next phase of digital transformation will depend not only on expanding connectivity but also on strengthening its capacity to govern, secure, and derive strategic value from digital assets. While investments in digital infrastructure, innovation, artificial intelligence, and e-government have positioned Kenya as a continental digital leader, growing dependence on foreign technologies, external data ecosystems, and multinational platforms presents emerging risks to resilience, competitiveness, and policy autonomy. Kenya must therefore build trusted digital infrastructure, enhance data governance,

promote responsible artificial intelligence, strengthen cybersecurity, and develop indigenous technological capabilities while maintaining productive global partnerships. Achieving this vision requires a whole-of-government approach that aligns digital governance with national security, industrial development, education, research, and foreign policy. A comprehensive National Digital Sovereignty Strategy will enable Kenya to reduce strategic vulnerabilities, unlock opportunities in artificial intelligence and digital trade, create high-value employment, and consolidate its position as a leading force in Africa's digital transformation.

Recommendations

1. The Executive Office of the President

(i) Oversee the development and implementation of a National Digital Sovereignty Strategy by June 2027 that establishes binding targets for sovereign cloud adoption, R&D expenditure, advanced digital skills production, and local content in government IT procurement while maintaining strategic international technology partnerships.

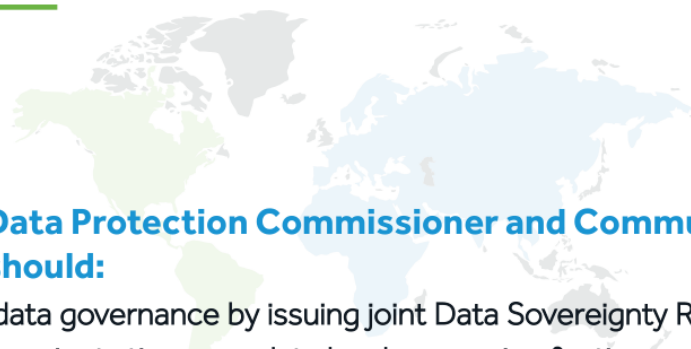
2. The Ministry of Information, Communications and the Digital Economy should:

(ii) Accelerate implementation of the Digital Superhighway Programme by prioritizing investment in a Tier III-certified Government Sovereign Cloud, establishing a National Data Centre in Konza Technopolis by 2028, and mandating security-cleared local hosting for all classified and personally identifiable government data.

(iii) Reinforce Kenya's digital ecosystem by introducing a "Kenya-First Digital" procurement preference for local technology enterprises in non-classified government contracts, mandating a minimum 30% local value addition in all ICT procurement above KSh 50 million, and creating enabling policies that increase participation of Kenyan firms in digital infrastructure, artificial intelligence, cybersecurity, and software development value chains.

(iv) Strengthen integrated governance frameworks for emerging technologies by introducing an Artificial Intelligence and Digital Platforms Bill that establishes mandatory algorithmic impact assessments for high-risk AI systems, requires platform transparency reports on content moderation and political advertising, and creates a civil liability regime for AI-related harms.





3. The Office of the Data Protection Commissioner and Communications Authority of Kenya should:

(v) Strengthen strategic data governance by issuing joint Data Sovereignty Regulations that classify government data into sovereignty tiers, mandate local processing for tier-one national security data, establish adequacy criteria for cross-border transfers, and require data protection impact assessments before deploying AI systems in the public sector.

(vi) Enhance oversight of digital platforms by jointly issuing Platform Accountability Regulations requiring quarterly transparency reports on content moderation decisions, algorithmic content curation parameters, and political advertising expenditure, with enforcement through graduated sanctions including financial penalties and service restriction.

(vii) Strengthen cybersecurity resilience by fully operationalizing the National Cyber Security Operations Centre, establishing sector-specific Computer Incident Response Teams in finance, energy, health, and telecommunications by 2027, and mandating bi-annual cybersecurity audits for operators of critical information infrastructure.

4. The National Treasury and the Ministry of Investments, Trade and Industry should:

(viii) Integrate digital sovereignty into Kenya's industrial development agenda by introducing a 150% enhanced deduction for qualifying expenditure on R&D in artificial intelligence, cybersecurity, cloud computing, and advanced software development, modeled on South Africa's Section 11D of the Income Tax Act.

(ix) Expand innovation financing mechanisms by capitalizing a Digital Sovereignty Venture Fund with KSh 5 billion in matching funds to de-risk private investment in local cloud services, AI startups, and cybersecurity enterprises, and directing the Kenya Development Corporation to establish a technology financing window.

5. The Ministry of Education, the Higher Education Sector, TVET Institutions and the National Research Fund should:

(x) Strengthen national capabilities in frontier technologies by funding 2,500 postgraduate scholarships annually in artificial intelligence, cybersecurity, and data science by 2028, requiring all public universities to establish dedicated AI and cybersecurity research centers, and integrating compulsory digital literacy into all TVET programs.

(xi) Promote university-industry collaboration by requiring industry co-funding for all National Research Fund grants exceeding KSh 20 million in digital technology fields, establishing a Technology Transfer Office in every public university with engineering or computer science faculties, and creating a Presidential Innovation Fellowship placing technology graduates in government agencies.





6. The Ministry of Foreign and Diaspora Affairs should:

(xii) Promote African collective digital sovereignty by establishing a dedicated Digital Diplomacy Directorate with specialized technology attachés in Brussels (AU/EU), Geneva (UN/ITU/WIPO), and Washington D.C. by 2028, and convening an annual African Digital Sovereignty Forum to coordinate continental positions on AI governance, data flows, and platform regulation.

7. The National Security Council and Relevant Security Institutions should:

(xiii) Integrate digital resilience into national security planning by mandating the National Intelligence Service to establish a National AI Security Assessment Centre, conducting a comprehensive vulnerability audit of all critical information infrastructure within 18 months, and developing coordinated responses to AI-enabled cyber threats, digital influence operations, and emerging technology risks.

(xiv) Establish stronger collaboration between security institutions, technology companies, research institutions, and regulators by institutionalizing a biannual National Digital Security Executive Briefing and conducting joint simulation exercises on AI-enabled threat scenarios, while ensuring oversight mechanisms that protect constitutional rights and democratic institutions.



THE GLOBAL CENTRE FOR POLICY AND STRATEGY
(GLOCEPS)

Research | Knowledge | Influence

Off Kiambu Road, Nairobi Kenya
P.O. Box 27023-00100, Nairobi.
Telephone: 011 2401331
Mobile: +254 700 279635
Email: info@gloceps.org
Web: <https://www.gloceps.org>

