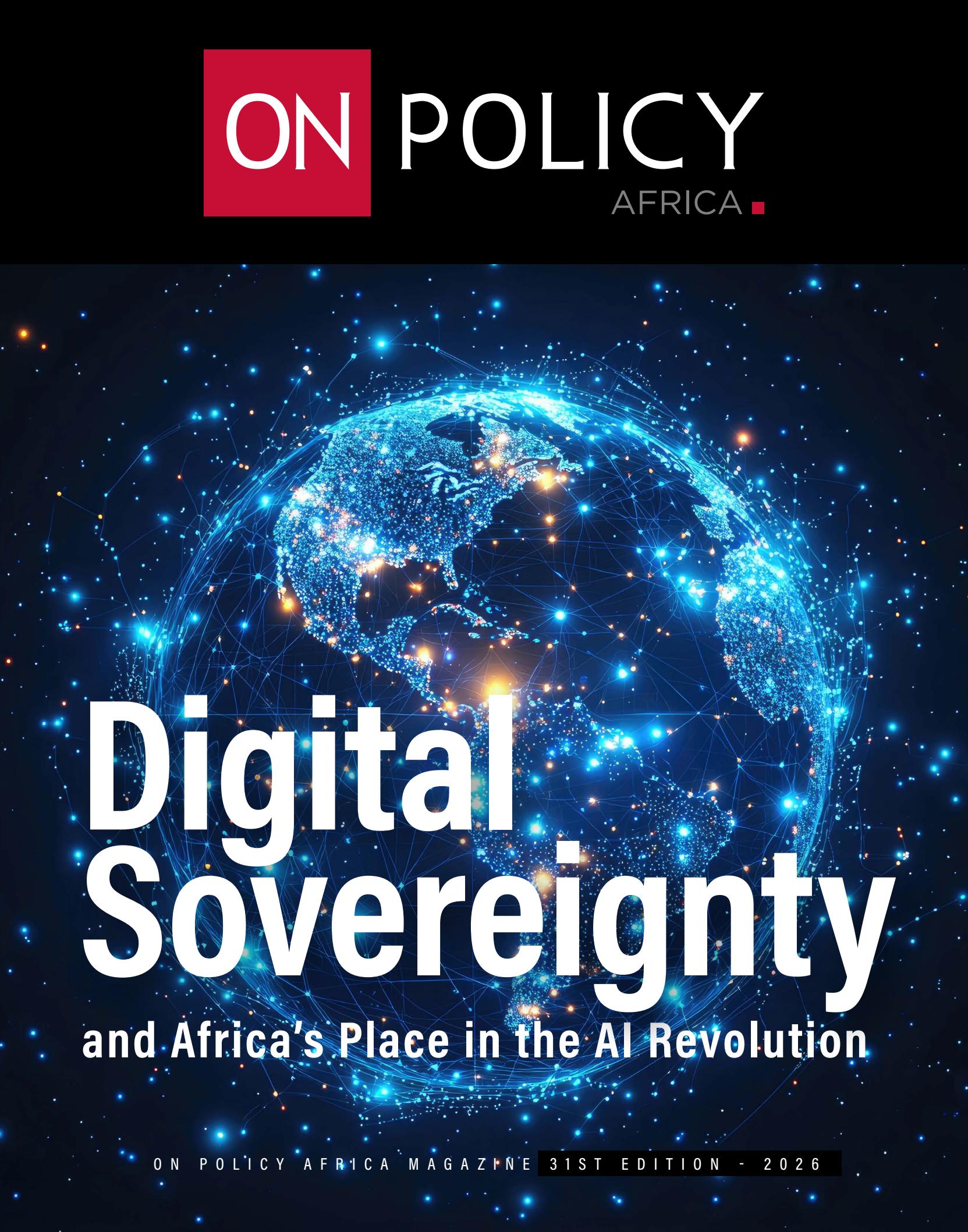


ON

POLICY

AFRICA ■



Digital Sovereignty

and Africa's Place in the AI Revolution

ON POLICY AFRICA MAGAZINE 31ST EDITION - 2026



“AI presents enormous opportunities for our continent.”

Lerato Mataboge

Editorial Team

EDITOR IN CHIEF

Mr Anthony Antem - *Head of Conflict Prevention and Analysis Unit, Nkafu Policy Institute*

SUPERVISION

Dr Julienne Mesumbe - *Deputy Director, Nkafu Policy Institute*

ADVISORY BOARD

Dr Denis Foretia - *Co-Chair, Denis and Lenora Foretia Foundation*

Mrs Lenora Ebule - *Co-Chair, Denis and Lenora Foretia Foundation*

CONTRIBUTORS

Dr Pippie Hughues - *Governance and Democracy Policy Analyst, Nkafu Policy Institute*

Dr Salim Ahmed Vessah - *Economic Policy Analyst, Nkafu Policy Institute*

Ms Larisa Ntoubia - *Research Assistant, Economic Affairs Division, Nkafu Policy Institute*

Mr Yesom Nwotazeh Jones - *Affiliate, Global Health Systems Solutions, GHSS*

Ms Muriel Kinkoh - *Research Associate, Nkafu Policy Institute*

Dr Solange Dabou - *Policy Analyst, Health Policy and Research Division, Nkafu Policy Institute*

Mr Musa Nji - *Policy Analyst, Health Policy and Research Division, Nkafu Policy Institute*

Mr Patrick Iskandar - *Policy Analyst, Health Policy and Research Division, Nkafu Policy Institute*

Prof. Theophile Nguimfack - *Fellow, Governance and Democracy Division, Nkafu Policy Institute*

Prof. Ngo Tong Chantal - *Fellow, Governance and Democracy Division, Nkafu Policy Institute*

Mr Enowbachem Agbortanyi - *Policy Analyst, Peace and Security Division, Nkafu Policy Institute*

DESIGN/LAYOUT

Mr Epoh Severin - *Head of Artistic and Visual Communication, Denis and Lenora Foretia Foundation*

Mr Ndze Alfred Steve - *Graphic Designer, Denis and Lenora Foretia Foundation*

Mr Nguene Edgar - *Graphic Designer, Denis and Lenora Foretia Foundation*

DIGITAL & COMMUNICATIONS TEAM

Mr Bruno Ittia - *Director of Communications and Strategic Initiatives, Denis and Lenora Foretia Foundation*

Mr Ayukmba Nkongonyor - *Deputy Director of Communications, Denis and Lenora Foretia Foundation*

Mr Davila Djomou Sumo - *Webmaster, Denis and Lenora Foretia Foundation*



ON POLICY AFRICA
www.onpolicy.org
info@onpolicy.org

Editorial Note

Digital Sovereignty and Africa's Place in the AI Revolution

Economic Features



Cloud Infrastructure: The Missing Foundation of Regional Integration in Central Africa Dr. Salim Vessah

Cloud infrastructure remains the overlooked backbone of regional integration in Central Africa, underpinning cross-border data flows, digital trade, and institutional interoperability essential for a cohesive and competitive regional economy



Advancing Regional Digital Sovereignty: Policy Responses to AI-Driven Data Colonialism in Africa Larissa Ntoubia

Advancing regional digital sovereignty in Africa requires coordinated policy responses to AI-driven data colonialism, ensuring that data governance, infrastructure, and innovation ecosystems are locally controlled, equitably governed, and aligned with the continent's long-term development priorities.



Artificial Intelligence Potential to Prevent Online Payment Fraud in Cameroon.

Yessom Nwotazeh Jones

Harnessing artificial intelligence to combat online payment fraud in Cameroon offers a transformative pathway to strengthen financial security, enhance real-time risk detection, and build greater trust in the country's rapidly expanding digital economy.

Perspectives on Health

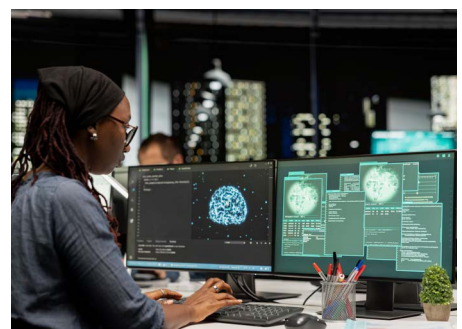
How AI Regulatory Sandboxes Can Accelerate Health Innovation in Africa Dr. Solange Dabou

AI regulatory sandboxes offer a pragmatic pathway to accelerate health innovation in Africa by enabling safe, real-world testing of emerging technologies while ensuring adaptive oversight, faster approvals, and context-responsive solutions.

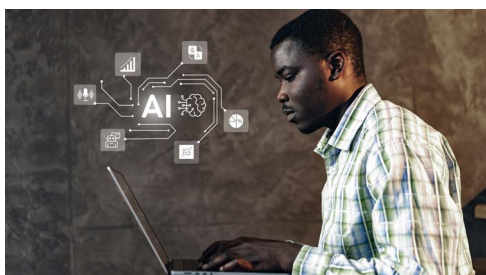


Neuroeconomics and digital sovereignty Musa Nji and Iskandar Patrick

Integrating neuroeconomics into digital sovereignty frameworks offers Africa a forward-looking strategy to safeguard cognitive autonomy in the AI economy, ensuring that algorithmic systems respect human decision-making processes while aligning technological development with the continent's social and ethical priorities.

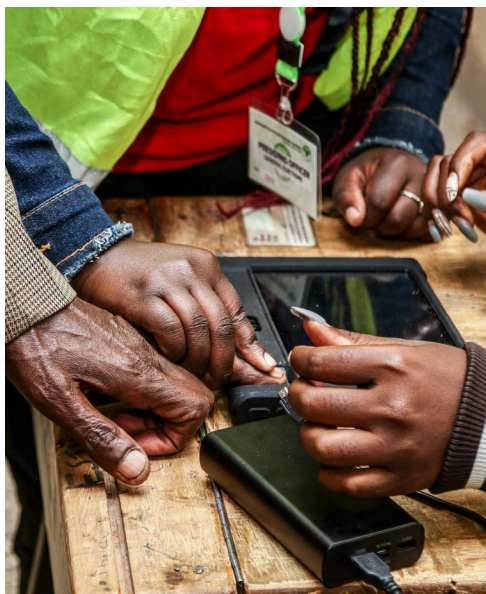


Governance features



The State: Actor or Regulator in the Promotion of Artificial Intelligence in Africa? Prof. Nguimfack Theophile

In Africa, the promotion of artificial intelligence calls for a government that acts as both a strategist and a regulator, capable of stimulating innovation while ensuring an ethical, inclusive framework conducive to sovereign technological development



Artificial intelligence, disinformation and political (in)stability in Cameroon Prof. Ngo Tong Chantal

Advancing regional digital sovereignty in Africa requires coordinated policy responses to AI-driven data colonialism, ensuring that data governance, infrastructure, and innovation ecosystems are locally controlled, equitably governed, and aligned with the continent's long-term development priorities.

Navigating Global AI Geopolitics: Africa's Role and Strategic Responses. Dr. Pippie Hughues

As global AI geopolitics intensify, Africa must assert a strategic role by shaping inclusive governance frameworks, strengthening regional alliances, and leveraging its data and talent to negotiate equitable participation in the evolving digital order.

Highlights on Peace and Security

Digital Authoritarianism and Electoral Security in Africa: Regulating Disinformation Without Curtailing Civic Space Enowbachem Agbortanyi

Balancing electoral security and civil liberties in Africa requires nuanced regulation of digital disinformation that counters authoritarian misuse of technology while safeguarding open civic space and democratic participation.



Optimizing Artificial Intelligence for Conflict Prevention in Africa: The case for Multilateral Cooperation and Localized Innovation Anthony Antem

Optimizing artificial intelligence for conflict prevention in Africa requires a dual focus on multilateral cooperation and localized innovation, enabling context-sensitive early warning systems while fostering coordinated, cross-border responses to emerging security threats.

Closing Insight

Policy Takeaways Across the Issue

**“Without AI
sovereignty,
Africa risks digital
colonisation.”**

Andile Ngcaba - itweb



Digital Sovereignty and Africa's Place in the AI Revolution

By Dr. Julienne Stéphanie Mesumbe

Africa's engagement with the artificial intelligence (AI) revolution is unfolding at a decisive moment, one in which data, algorithms, and digital infrastructure are rapidly becoming the new foundations of economic power, governance capacity, and geopolitical influence. As AI systems increasingly shape financial transactions, political communication, health delivery, and security operations, the question for African countries is no longer whether to adopt AI, but under what conditions, through whose systems, and in whose interests such technologies are deployed. At the center of this debate lies digital sovereignty: the ability of states and regions to exercise meaningful control over their data, digital infrastructure, and innovation pathways.

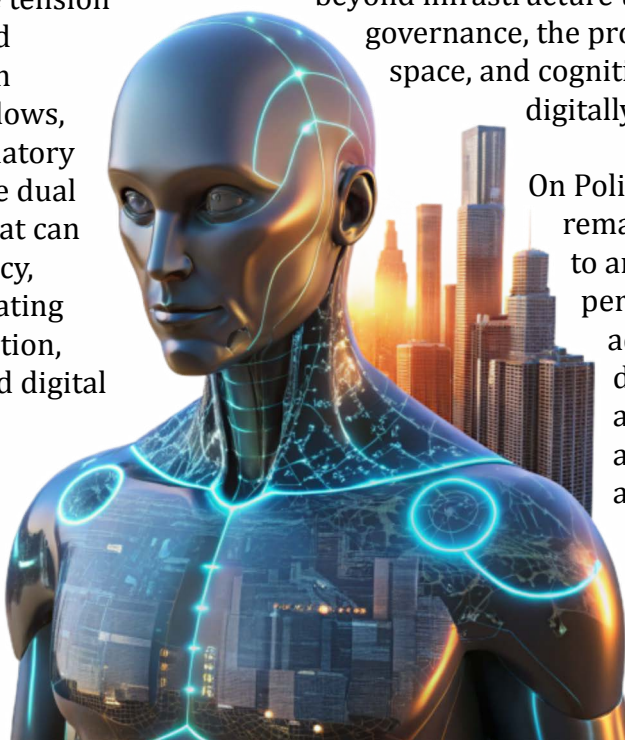
For much of the continent, AI adoption is taking place within a global digital architecture that remains largely designed, owned, and governed outside Africa. Cloud infrastructure, data centers, leading platforms, and many of the standards that shape AI development are still concentrated in a few global power centers. These tools offer real opportunities for growth, service delivery, and improved efficiency. Yet they also reproduce deep asymmetries that risk locking African countries into new forms of dependency, where data is extracted, processed, and monetized elsewhere, and where national policy choices are constrained by external technological control. In this context, digital sovereignty is no longer a distant aspiration or a purely normative idea; it has become a practical

requirement for protecting autonomy, resilience, and long-term development.

This thirty-first issue of On Policy Magazine examines Africa's place in the AI revolution through a multidisciplinary lens spanning economics, governance, health, peace, and security. Across the contributions, three central tensions emerge. The first is the tension between innovation and sovereignty: how African countries can harness AI's transformative potential without deepening dependence. The second is the tension between global integration and regional control, particularly in relation to cross-border data flows, cloud infrastructure, and regulatory harmonization. The third is the dual nature of AI itself, as a force that can enhance efficiency, transparency, and prevention, while also creating new risks linked to disinformation, surveillance, manipulation, and digital authoritarianism.

The issue opens by grounding the debate in the political economy of digital infrastructure, positioning cloud systems not as a technical afterthought but as the silent foundation of regional integration and digital sovereignty. It then explores how AI is reshaping financial systems and public service delivery, while revealing regulatory gaps that leave societies vulnerable to fraud, data extraction, and ethical abuse. The governance and security sections examine AI's stabilizing and destabilizing potentials, especially in elections, information ecosystems, and conflict prevention, underscoring the urgent need for rights-based regulation, institutional capability, and coordinated oversight.

A unifying message runs through the issue: Africa cannot become a meaningful actor in the AI era without coordination, capacity, and investment at scale. National strategies are necessary, but insufficient on their own. Digital sovereignty requires regional approaches: interoperable data governance regimes, harmonized regulatory frameworks, shared digital infrastructure, and innovation ecosystems that are owned and shaped locally. It also requires a deeper recognition that sovereignty extends beyond infrastructure to include ethical governance, the protection of civic space, and cognitive autonomy in digitally mediated societies.



On Policy Magazine remains committed to amplifying African perspectives and advancing policy debates that place agency, equity, and sustainability at the center of technological transformation. This issue brings together voices from across the Nkafu Policy Institute and beyond to

demonstrate that Africa's response to the AI revolution will not be judged by speed of adoption alone, but by the degree to which AI is aligned with the continent's values, development priorities, and democratic aspirations. The choices made today, on data governance, infrastructure ownership, and AI governance, will determine whether Africa remains a passive consumer of digital power or emerges as an active architect of its digital future.

Cloud Infrastructure: The Missing Foundation of Regional Integration in Central Africa

Cloud infrastructure remains the overlooked backbone of regional integration in Central Africa, underpinning cross-border data flows, digital trade, and institutional interoperability essential for a cohesive and competitive regional economy

By Dr. Salim Vessah

When Central Africa's Data Is Stored Abroad

Entrepreneurs in Douala, Cameroon utilize platforms hosted in Europe. A start-up in Libreville stores its data in South Africa. A public administration in Bangui relies on servers located outside the continent for its digital services. These various, often overlooked realities highlight a fundamental yet frequently ignored issue: the digital economy in Central Africa primarily depends on infrastructure situated elsewhere. If this

is the case, can we truly discuss regional integration when data the driving force of the modern economy is stored, processed, and controlled outside the region? This question may initially seem technical, but it is, in fact, deeply economic and strategic. Today, data serves the economy much like roads and ports did in the industrial era: as essential infrastructure.



CREDIT: VECTEEZY

The Missing Link in Central African Integration

For decades, regional integration has been portrayed as the ultimate solution to the structural constraints facing Central African economies, such as small domestic markets, dependence on raw materials, landlocked status, and inadequate, often poor-quality infrastructure. Yet, despite the rhetoric, the establishment of regional institutions and the signing of numerous treaties, intra-regional trade in Central Africa still accounts for less than 10% of total trade, compared to over 60% in Europe and around 40% in East Asia. This low level of integration

is often attributed to customs barriers, the lack or poor quality of transport infrastructure, and various political constraints. However, another, less visible dimension now plays an equally important role: digital infrastructure. Modern economic integration relies on countries' ability to connect their payment systems, public administrations, businesses, and digital platforms. Without adequate cloud infrastructure, this digital integration remains limited, slow, and costly. The central issue, therefore, is this: Central Africa is in a challenging position, attempting to build economic integration in the 21st century with insufficient digital infrastructure.

Why Cloud Infrastructure Is an Economic Issue, Not Just a Technical One

The first argument is economic: the lack of local cloud infrastructure contributes to high transaction costs. In Africa, the cost of broadband accounts for approximately 4–5% of average monthly income, compared to less than 1.5% in developed economies. For SMEs, this limits access to digital services, e-commerce, and regional platforms. However, in regions where digital systems are well integrated, the digitization of commercial procedures has reduced transaction times by 30% to 50%, directly stimulating trade.

The second argument concerns competitiveness: when a Central African company hosts its data in Europe or South Africa, it incurs higher costs, experiences delays, faces longer latency times, and relies on foreign infrastructure. On a larger scale, this reduces the competitiveness of the entire region and hampers the development of the digital economy.

The third argument addresses financial inclusion and innovation, with Kenya providing a telling example. The development of digital infrastructure and data centers has fueled the growth of fintech and mobile financial services. Today, over 80% of the population has access to digital financial services.

This transformation has facilitated trade, supported entrepreneurship, and attracted technological investment, making Nairobi a regional

technology hub. Similarly, **South Africa** has established itself as a continental cloud hub, thanks to massive investment in data centers, attracting major technology companies while stimulating local innovation.

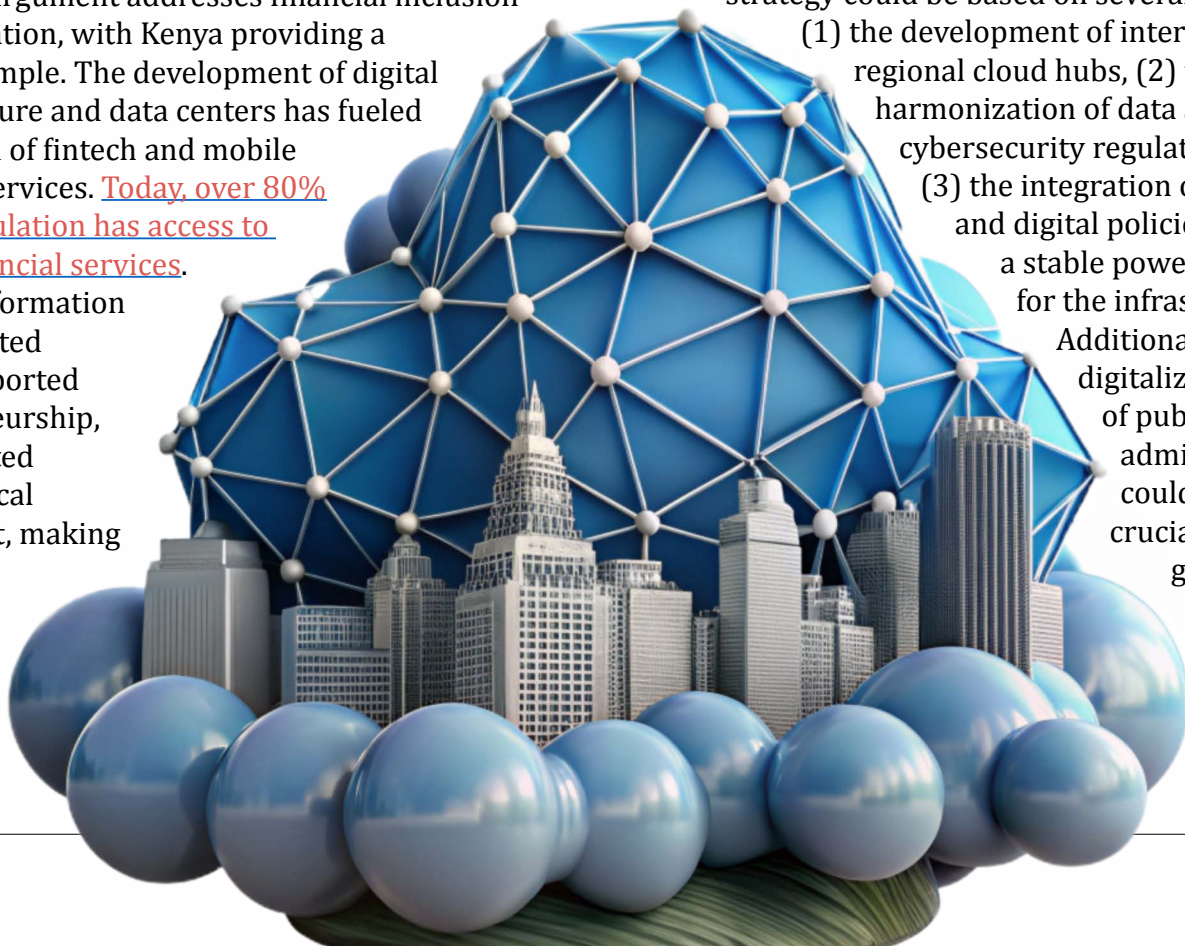
These examples clearly demonstrate that cloud infrastructure is not merely a technological issue but a strategic economic asset essential for achieving long-term integration goals. Consequently, countries that invest in this infrastructure become digital hubs, while others become increasingly dependent.

Think Regional, Not National

Today, the question is no longer whether Central Africa should invest in cloud infrastructure, but rather how to do so effectively. A purely national approach would face significant limitations, as markets are often too small to make large data centers profitable. In contrast, a sub-regional or regional approach would allow costs to be shared, attract multiple investors, and create a genuine regional digital market. Therefore, a regional

strategy could be based on several pillars:

- (1) the development of interconnected regional cloud hubs, (2) the harmonization of data and cybersecurity regulations, and (3) the integration of energy and digital policies to ensure a stable power supply for the infrastructure. Additionally, the digitalization of public administrations could play a crucial role by generating local demand for cloud



services. If this strategy is well coordinated, cloud infrastructure could become for Central Africa what ports and railways have been for other regions: a true catalyst for economic integration.

Cloud Infrastructure as the New Foundation of Regional Integration

In the 21st century, integration in Central Africa cannot be limited to roads, borders, and physical trade; it must also encompass data, digital platforms, and cloud infrastructure. Without this infrastructure, the region risks disaster and may be sidelined in the digital economy, a cornerstone of the African Continental Free Trade Area. The cloud is not just a technology; it is a strategic tool. For Central Africa, it could serve as the invisible yet essential foundation for tomorrow's regional integration. Therefore, the real question for decision-makers is not whether to invest in the cloud, but whether they can afford not to. With this in mind, three priority actions can be implemented immediately:

Launch two or three regional cloud hubs: Identify host countries, secure funding from international partners, and attract private operators.

The goal is to create a regional, rather than national, infrastructure.



*... integration
in Central
Africa cannot
be limited
to roads,
borders, and
physical
trade; it
must also
encompass
data, digital
platforms,
and cloud in-
frastructure.*

Harmonize digital regulations across countries: Adopt common rules on data, cybersecurity, and digital payments to facilitate business operations throughout the region.

Digitize public services to create demand: Customs, taxation, digital identity, and public payments must be digitized and hosted locally. This will position the state as the regional cloud's first customer and attract private investment.

Thus, regional integration will not be achieved solely through trade agreements but through digital infrastructure. In an era marked by the fragmentation of geopolitical and economic blocs globally, regions that control their data will build economic power, while others will depend on them.



CREDIT: MAGNIFIC.COM

Advancing Regional Digital Sovereignty:

Policy Responses to AI-Driven Data Colonialism in Africa

Advancing regional digital sovereignty in Africa requires coordinated policy responses to AI-driven data colonialism, ensuring that data governance, infrastructure, and innovation ecosystems are locally controlled, equitably governed, and aligned with the continent's long-term development priorities.

By Larissa Ntoubia

Artificial intelligence (AI) is rapidly transforming global economic and political systems, redefining how data is produced, governed, and used for innovation and development. As major global powers invest heavily in AI capabilities and digital infrastructure, the issue of digital sovereignty, which is the ability of states

to control and govern their digital ecosystems, has become a priority. In Africa, the [Continental Artificial Intelligence Strategy](#) enacted by the African Union in 2024, has a very transformative vision. The strategy aims to leverage AI to contribute [\\$1.5 trillion](#) to the continent's economy by 2030. The continent stands to gain transformative benefits in sectors

such as healthcare, finance, agriculture, and governance, yet it faces a pressing risk of becoming a passive consumer of AI technologies controlled by foreign entities. This reliance exposes African nations to what is known as AI-driven data colonialism, where critical data is extracted and monetized abroad, often with minimal benefits to local communities. This paper highlights why regional digital sovereignty is critical and outlines practical steps for African countries to assert control over AI.

The Challenge of Regional Digital Dependence

Across Africa, the majority of AI applications and cloud services are hosted on several platforms, managed by companies based in the United States, Europe, and China. The continent accounts for [about 1%](#) of total available global data center capacity, despite hosting 19.1% of the world's population. This concentration of data and technological capacity outside African borders limits national supervision and reduces the continent's ability to use AI for development. Also, current regulatory frameworks are fragmented. While countries like [Nigeria, Kenya, and South Africa](#) have enacted data



*Across Africa,
the majority
of AI
applications
and cloud
services
are hosted
on several
platforms,
managed by
companies
based in the
United States,
Europe, and
China.*

protection laws, these statutes vary widely in scope and enforcement.

Moreover, there is an imbalanced data flow, where foreign technology companies dominate digital platforms and extract vast amounts of user data from social media, search engines, and applications that require the protection of personal data. Initiatives such as Free Basics Facebook, which provide subsidized internet access, further promotes this dynamic by capturing user metadata and shaping online experiences toward predominantly Western content. As a result, data generated in Africa is exported and leveraged to [drive innovation and profits elsewhere](#), widening the digital and economic divide. The [Cambridge Analytica scandal](#) illustrates the risks of this system, where Facebook user data was exploited for political manipulation and external interests, highlighting the broader implications of weak data governance and foreign control over Africa's digital ecosystem. Cross-border digital flows often bypass national or regional supervision mechanisms, leaving African governments with little leverage to enforce ethical practices or ensure local economic benefits. This creates



CREDIT: TIKSA NEGERI/REUTERS

an environment in which foreign corporations dictate digital norms, effectively shaping Africa's technological trajectory without African input.

Policy Pathways for Action

Many African countries still lack clear AI and data governance policies; [only 22](#) out of 54 African countries have national AI strategies as of 2026 compared to 16 in 2024 this points out an improvement in number. However, these figures still remain low. Governments should adopt these policies to establish accountability standards and enforce compliance among both foreign and domestic operators. Regional coordination under the African Union and AfCFTA frameworks have

provided the necessary starting point for regulations harmonization, ensuring consistency in cross-border data handling and promoting digital trade that benefits African stakeholders.

A Call for Coordinated Governance

Strengthening digital sovereignty cannot be achieved by individual countries acting alone. The AU and regional economic communities have a central role to play in harmonizing AI governance frameworks. A practical example of regional digital governance is the African Union Data Policy Framework, which guides member states on data governance and cross-border data flows. Likewise, AfCFTA's Protocol on Digital Trade provides a foundation for harmonizing

digital regulations across African markets. Together, these initiatives show how regional institutions can support coordinated digital sovereignty. This creates standards for data protection, and ensure interoperability across-borders. Coordinated governance allows African nations to speak with a unified voice in negotiating with international tech companies and setting the rules of engagement for AI deployment. Such harmonization is not merely a paper exercise. It directly affects economic competitiveness, national security, and the equitable distribution of benefits derived from AI.



CREDIT: VECTEEZY

Building Local AI Capacity

A cornerstone of digital sovereignty is the development of indigenous AI capabilities. Africa currently produces a small fraction of global AI research and development outputs, reflecting gaps in talent, infrastructure, and investment. Developing local AI ecosystems is essential not only for technological independence but also for ensuring that AI solutions are relevant to African contexts. Strategic investments in research centers, innovation hubs, and training programs can nurture a new generation of AI practitioners and entrepreneurs. Public-private partnerships, alongside incentives for local startups, can stimulate innovation and attract capital while keeping data and intellectual property within the continent. Strengthening local capacity ensures that Africa does not

simply consume AI products but actively shapes and deploys technology in ways that serve its own development priorities.

Conclusion

Africa's engagement with AI can accelerate development and make the continent take charge in a fast-changing digital world. AI-driven data colonialism represents a clear and urgent threat to the continent's sovereignty while underscoring the need for decisive, and coordinated policy action. By harmonizing regulations, building local capacity, and fostering ethical AI use, African countries can protect their digital assets while positioning themselves as active, and competitive participants in the global AI landscape. Advancing regional digital sovereignty is not a distant aspiration it is essential to determining whether Africa shapes its own technological future or remains subject to external control.

“
AI-driven
data
colonialism
represents
a clear
and urgent
threat to the
continent's ...

Artificial Intelligence Potential to Prevent Online Payment Fraud in Cameroon

Harnessing artificial intelligence to combat online payment fraud in Cameroon offers a transformative pathway to strengthen financial security, enhance real-time risk detection, and build greater trust in the country's rapidly expanding digital economy.

By Yessom Nwotazeh Jones

Introduction

Cameroon incurred over 1 billion FCFA loss to [online payment fraud in 2025](#). These losses resulted from the following scams; phishing through fake email, SMS or website impersonation, mobile money fraud through fake credit/debit alert, wrong transfer scam, WhatsApp impersonation, fake job/freelance payment scams, prize/lottery scams, fake social media vendors, SIM swap fraud, advance-fee fraud, account takeover and, [Ponzi schemes](#). The losses incurred over the years shows an upward fraud trajectory with 2023 marked the peak of digital fraud in Cameroon. The fraud networks were well structured, evident of

widespread Ponzi schemes. An estimated [7 billion FCFA lost to cyber-crime over a period from 2010 to 2023](#). The victims were individuals, businesses and, government agencies. Victims are tricked into providing their passwords, PIN, banking details, other personal information or exploit the trust relationship and demand urgent transfer. This results in financial hardship, stress, compromise of personal data and, disruption in business operations due to cyber-attacks. If not put under control, it will reduce public trust in state institutions. The aim of this paper is to sensitize the public, provide a way-forward to curb digital fraud and build public trust in Cameroon and Africa.



CREDIT: VECTEEZY

Government Intervention

Government crackdown on Ponzi schemes resulted to a reduction in fraud related losses in 2025. The government has promulgated into Law, a criminal act. Law N^o 2010/012 of 12 December 2010 on cyber criminality stipulates that criminal investigation of this nature shall be the sole responsibility of [judicial police trained in digital forensics](#).

The National Agency for Information and Communication Technologies (ANTIC) in 2025 identified 59 scam platforms, shutdown 40. Also, 4781 fake social media accounts of which 3466 were blocked. 471 scam cases and [5973 vulnerable cases were identified](#). Despite these efforts, Antic faces inadequate skilled personnel to handle matters of digital forensics. However, the AI algorithm is holistic, can shut down all possible tactics by fraudsters and solve the personnel problem. This leads us to the importance of adopting AI into the regulatory system.

The Role of AI in Fraud Detection and Prevention

AI algorithms can handle the adaptive nature and scale of digital fraud. In Kenya, the banking and mobile money sector experienced significant reduction in fraud incidents after AI application. 65% of banks apply AI for credit risk scoring. For MPesa AI applied in real time fraud detection and risk scoring handles up to [12000 transactions per second](#).

AI changes the game from rule-based systems to AI algorithms that sort out irregular transaction patterns, detect account hacking attempts, predict phishing messages, detect the next move of fraud networks and prevent future fraud threats. AI can send warning signals alerting the user of potential fraud attack. In Nigeria, about 37% of Fintech apply AI to credit scoring and risk modeling, 62.5% use [AI-powered chatbots for customer retentions](#).

However, the misuse of AI can enhance digital fraud by personalizing emails or SMS, deep fake and voice cloning attacks, by pass captcha and basic fraud detection systems, generate fraudulent accounts and creating malware to evade detection systems. Because AI can perform all this, only proves it understands how the system works and has the capacity to beat it.

Recommendations

Policy makers should adopt an AI framework for real - time transaction screening, update privacy and data protection policies, be transparent on who takes the fall for AI errors and, adopt AI cyber security measures for finance institutions.

- Government should build a single fraud database to secure data sharing.
- Equip ANTIC with centralized AI monitoring systems to ease fraud prediction.

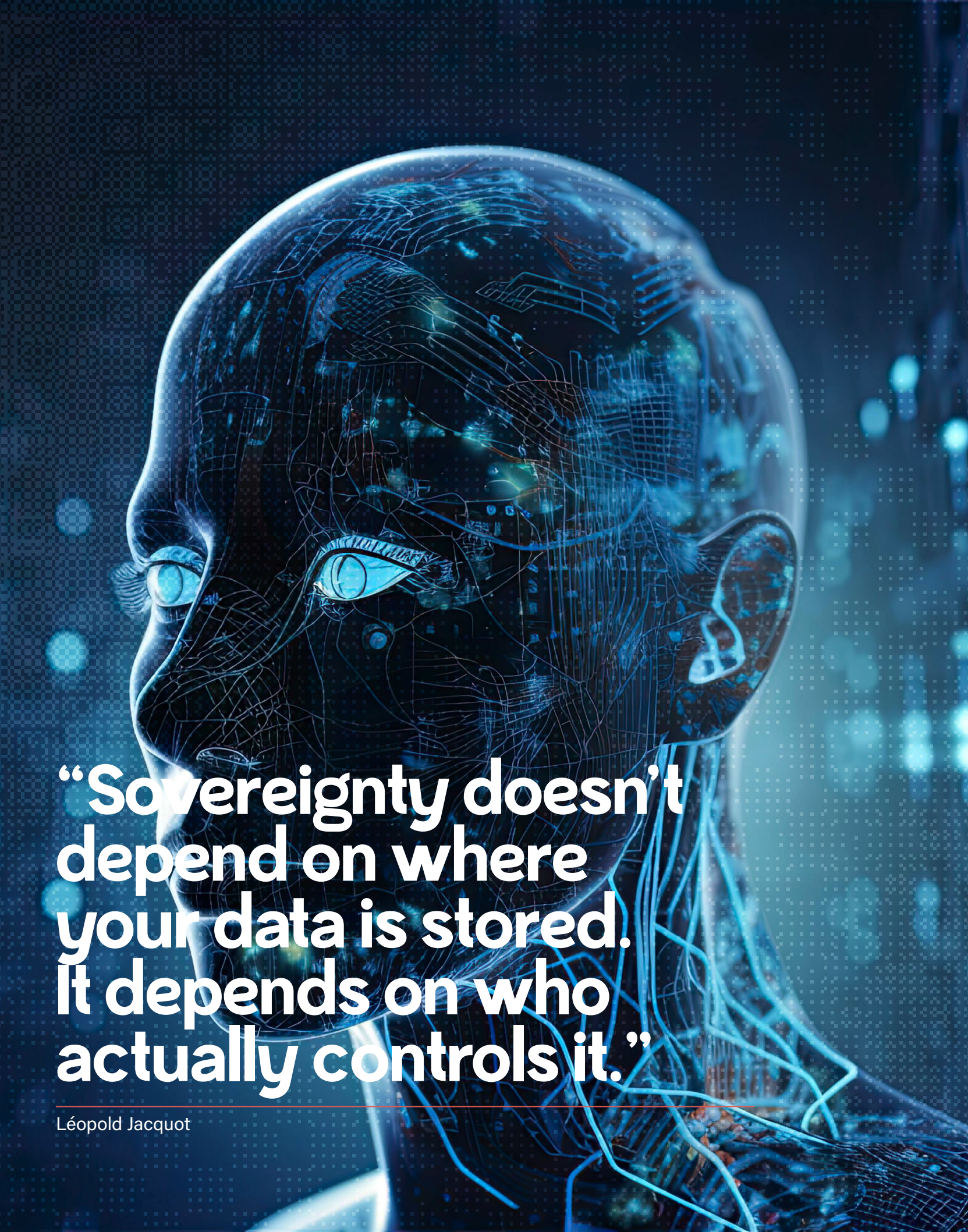


*AI can send
warning
signals
alerting
the user of
potential
fraud attack.*

- Banks and telecom providers should adopt real-time AI fraud monitoring to ease fraud detection.
- Adopt AI principles that focus on safeguarding and privacy in order to strengthen data protection.

Conclusion

Though AI misuse can enhance fraud, it remains the best technology to prevent online payment fraud and beat scammers at their own game. By adopting AI into the regulatory system, ANTIC will have the capacity to predict, securely share, detect and prevent online fraud and threats. Without a robust sovereign AI fraud prevention framework, both public trust and digital sovereignty would be compromise.



**“Sovereignty doesn’t
depend on where
your data is stored.
It depends on who
actually controls it.”**

Léopold Jacquot

How AI Regulatory Sandboxes Can Accelerate Health Innovation in Africa

AI regulatory sandboxes offer a pragmatic pathway to accelerate health innovation in Africa by enabling safe, real-world testing of emerging technologies while ensuring adaptive oversight, faster approvals, and context-responsive solutions

By Dr. Solange Dabou

Artificial Intelligence (AI) is transforming our societies, creating untold opportunities but also unprecedented challenges. AI and Machine Learning (ML) are [revolutionizing health research and practice](#), from health system management to personalized medicine through predictive models for public health, innovation in diagnostics and drug discovery, clinical decision support and new approaches to healthcare. [In Africa](#), AI-driven tools hold strong potential to address persistent health system challenges such as shortages of healthcare workers, limited infrastructure and equipment, delayed diagnostics, and weak health information systems.

However, while AI is constantly expanding the limits of what is possible, regulatory frameworks often struggle to adapt, sometimes relying on outdated frameworks outpaced by the fast-moving advances in technology. AI governance challenges in Africa are complex and create uncertainty for both innovators and policymakers. To ensure African health innovations can flourish while complying with legislations and consumer rights, governance frameworks must adapt and evolve. [Regulatory sandboxes](#) are emerging as a practical way to enable the safe testing of new technologies under controlled conditions and should be considered a key instrument for promoting the responsible and



*Originating
from the
fintech
ecosystem, AI
sandboxes
are gaining
momentum
in Africa
but remain
unevenly
developed...*

ethical development and deployment of AI-driven health solutions.

Regulatory Gaps in AI Governance in Africa

[AI systems rely on data to learn, adapt, and create](#)

[value](#). The AI governance issue is therefore a data governance issue. Data governance can be defined as the [system used by institutions and organizations](#) to manage data responsibly across its lifecycle, ensuring it is used safely, ethically, and in line with the law while delivering value to stakeholders. In healthcare and health research, AI governance also requires careful consideration of [Ethical, Legal and Societal Implications](#) (ELSI) of AI tools and ML models. This includes ensuring that AI systems uphold principles of patient safety, fairness, accountability, transparency, equity and real-world impact on health systems. AI and data governance in Africa are constrained by fragmented regulatory frameworks, weak data protection and accountability systems, and limited institutional capacity to oversee AI deployment effectively. Many existing AI policies and models are imported or adapted from global frameworks that do not fully reflect [African socio-economic realities](#), cultural values, or health system needs, leading to misaligned or ineffective implementation. Existing data governance structures increase the risk of digital colonialism, where data generated in Africa is extracted, processed, and monetized by external actors with [limited local control or benefit-sharing](#). Furthermore, limited technical expertise [among regulators](#), gaps in coordination and inadequate stakeholder engagement hinder effective oversight and trust-building.

AI Regulatory Sandboxes

Originating from the fintech ecosystem, AI sandboxes are gaining momentum in Africa but remain unevenly developed, with the few existing initiatives still in early or experimental stages.

What it is and how it works

[AI regulatory sandboxes](#) are structured, time-bound environments that allow innovators, regulators, and other stakeholders to test AI technologies



CREDIT: MAGNIFIC.COM

in real-world conditions under regulatory supervision, without immediately being subject to the full force of existing regulations. Rather than bypassing the law, sandboxes create a controlled space for experimentation and learning, enabling governments to better understand emerging AI systems while developers receive guidance on how regulations apply in practice.

The Datasphere initiative categorizes sandboxes into three main forms: operational (testing technical performance and data flows), regulatory (testing compliance under regulatory guidance), and hybrid (combining technical testing with legal learning).

AI regulatory sandboxes operate through a structured, time-bound process that allows safe experimentation with new technologies. Regulators define a clear scope and select eligible innovators, who then test AI systems in controlled real-world or simulated settings. Throughout the process, regulators and developers engage in continuous dialogue, using lessons from testing to refine products, clarify regulatory expectations, and inform future rules. At the end of the sandbox, solutions either scale, adapt, or exit, while regulators retain evidence to strengthen AI governance and policy design.

A Policy Tool to Enable Safe Health Innovation

[Traditional AI regulatory models](#) struggle to keep pace with AI-enabled health solutions, where risks, data uses, and performance often only become clear through real-world deployment. As a result, promising health innovations may be delayed, blocked, or deployed without adequate regulatory learning, increasing risks for patients and health systems. AI regulatory sandboxes offer a more agile and adaptive alternative. By allowing health technologies to be tested in controlled environments, sandboxes will enable early risk identification, iterative improvement, and evidence-based regulatory decision-making. Instead of waiting for innovation to mature before regulating, regulators and innovators learn together and improve both products and oversight. This approach is particularly valuable in healthcare, to balance rapid innovation and ELSI considerations. Where traditional models rely on a slow linear “Problem-Plan-Design-Develop-Implement” method, sandboxes offer a flexible collaborative and multistakeholder alternative. To maximize impact, three priorities stand out: [integrating sandboxes](#) into wider national and regional AI and health-data governance frameworks



*Where
traditional
models
rely on a
slow linear
“Problem-
Plan-Design-
Develop-
Implement”
method,
sandboxes
offer a flexible
collaborative
and
multistake-
holder
alternative.*

so they inform legal reform rather than operate in isolation; [building institutional and human](#) capacity to translate ethical AI principles into practice; and ensuring inclusive, multistakeholder participation, especially from [civil society](#) and health practitioners, to identify health-system risks and societal impacts early.

Conclusion

AI regulatory sandboxes offer Africa a timely opportunity to bridge the gap between rapid health innovation and adaptive governance. By creating supervised environments where AI-driven health solutions can be tested, refined, and understood before large-scale deployment, sandboxes help reduce regulatory uncertainty while safeguarding patient rights and public trust. Used strategically, they can accelerate the safe adoption of locally relevant AI solutions, ensuring Africa captures lasting value from its ongoing AI-driven health transformation.

Neuroeconomics and digital sovereignty:

Securing the cognitive autonomy of AI economy in Africa

Integrating neuroeconomics into digital sovereignty frameworks offers Africa a forward-looking strategy to safeguard cognitive autonomy in the AI economy, ensuring that algorithmic systems respect human decision-making processes while aligning technological development with the continent's social and ethical priorities.

By Musa Nji and Iskandar Patrick Abadoma Mounpou

Artificial intelligence (AI) is rapidly transforming global economic and political systems, redefining how data is produced, governed, and used for innovation and development. As major global powers invest heavily in AI capabilities and digital infrastructure, the issue of digital sovereignty, which is the ability of states

to control and govern their digital ecosystems, has become a priority. In Africa, the [Continental Artificial Intelligence Strategy](#) enacted by the African Union in 2024, has a very transformative vision. The strategy aims to leverage AI to contribute [\\$1.5 trillion](#) to the continent's economy by 2030. The continent stands to gain transformative benefits in sectors

clear through real-world deployment. As a result, promising health innovations may be delayed, blocked, or deployed without adequate regulatory learning, increasing risks for patients and health systems. AI regulatory sandboxes offer a more agile and adaptive alternative. By allowing health technologies to be tested in controlled environments, sandboxes will enable early risk identification, iterative improvement, and evidence-based regulatory decision-making. Instead of waiting for innovation to mature before regulating, regulators and innovators learn together and improve both products and oversight. This approach is particularly valuable in healthcare, to balance rapid innovation and ELSI considerations. Where traditional models rely on a slow linear “*Problem-Plan-Design-Develop-Implement*” method, sandboxes offer a flexible collaborative and multistakeholder alternative. To maximize impact, three priorities stand out: [integrating sandboxes](#) into wider national and regional AI and health-data governance frameworks

so they inform legal reform rather than operate in isolation; [building institutional and human](#) capacity to translate ethical AI principles into practice; and ensuring inclusive, multistakeholder participation, especially from [civil society](#) and health practitioners, to identify health-system risks and societal impacts early.

Conclusion

AI regulatory sandboxes offer Africa a timely opportunity to bridge the gap between rapid health innovation and adaptive governance. By creating supervised environments where AI-driven health solutions can be tested, refined, and understood before large-scale deployment, sandboxes help reduce regulatory uncertainty while safeguarding patient rights and public trust. Used strategically, they can accelerate the safe adoption of locally relevant AI solutions, ensuring Africa captures lasting value from its ongoing AI-driven health transformation.



CREDIT: MAGNIFIC.COM

A portrait of Yuval Noah Harari, a man with glasses and a dark jacket, against a dark blue background with a subtle grid pattern. The quote is overlaid in large white text.

**“There are
no longer
independent
countries but
data colonies.”**

Yuval Noah Harari

GOVERNANCE

The State: Actor or Regulator in the Promotion of Artificial Intelligence in Africa?

In Africa, the promotion of artificial intelligence calls for a government that acts as both a strategist and a regulator, capable of stimulating innovation while ensuring an ethical, inclusive framework conducive to sovereign technological development

By Prof. Ngumfack Théophile

No activity undertaken by the population escapes the control of the State. Artificial intelligence (AI) is no exception. Yet, one might think that AI is of interest only to the experts who develop it and its various users. However, this would be to overlook the impact of these new technologies on human life and State governance. In fact, AI refers to the branch of computer science that aims to simulate human cognitive abilities. It relies on the creation and application of algorithms executed in a dynamic computing environment, which enables computers [to think and act like human beings](#).

Thus, AI has a huge impact on how we go about our daily life in the society, how life is governed, and the role humans play within it. However, we must be careful that this technology does not turn against humanity. According to [the United Nations](#), while AI has the potential to address some of humanity's greatest challenges, its rapid development inevitably comes with a series of risks and challenges. These challenges call for an effective government strategy in promoting AI, particularly [in contexts where technological culture is not yet well-established, such as in Central Africa](#). Upon analysis, the State has

the responsibility to combine concrete actions and regulation in promoting AI. Furthermore, AI represents a challenge for State governance, because although it is a competing actor, it remains primarily a key regulator of this new technology.

I- Artificial intelligence, a challenge for State governance

AI is a technological advancement [that serves humanity](#). It is therefore logical that a State concerned with its development would see it as a governance issue at three levels at least.

At the economic level, promoting AI makes it possible to develop technologies that enhance [the performance of economic operators](#). This performance, in terms of productivity and efficiency, leads to additional wealth creation and an increased tax base.

At the social level, the technological innovations associated with artificial intelligence aim to improve the [living conditions of populations](#). The impact can be seen in fields such as healthcare, security, and trade.

At the level of governance in public and private organizations, AI has become a [decision-support tool](#). It saves time and helps reduce errors in task execution. Its applications are developed and used



*There can
be no AI
without a
government
policy
geared
towards
investments
that
structure the
digital sector.*

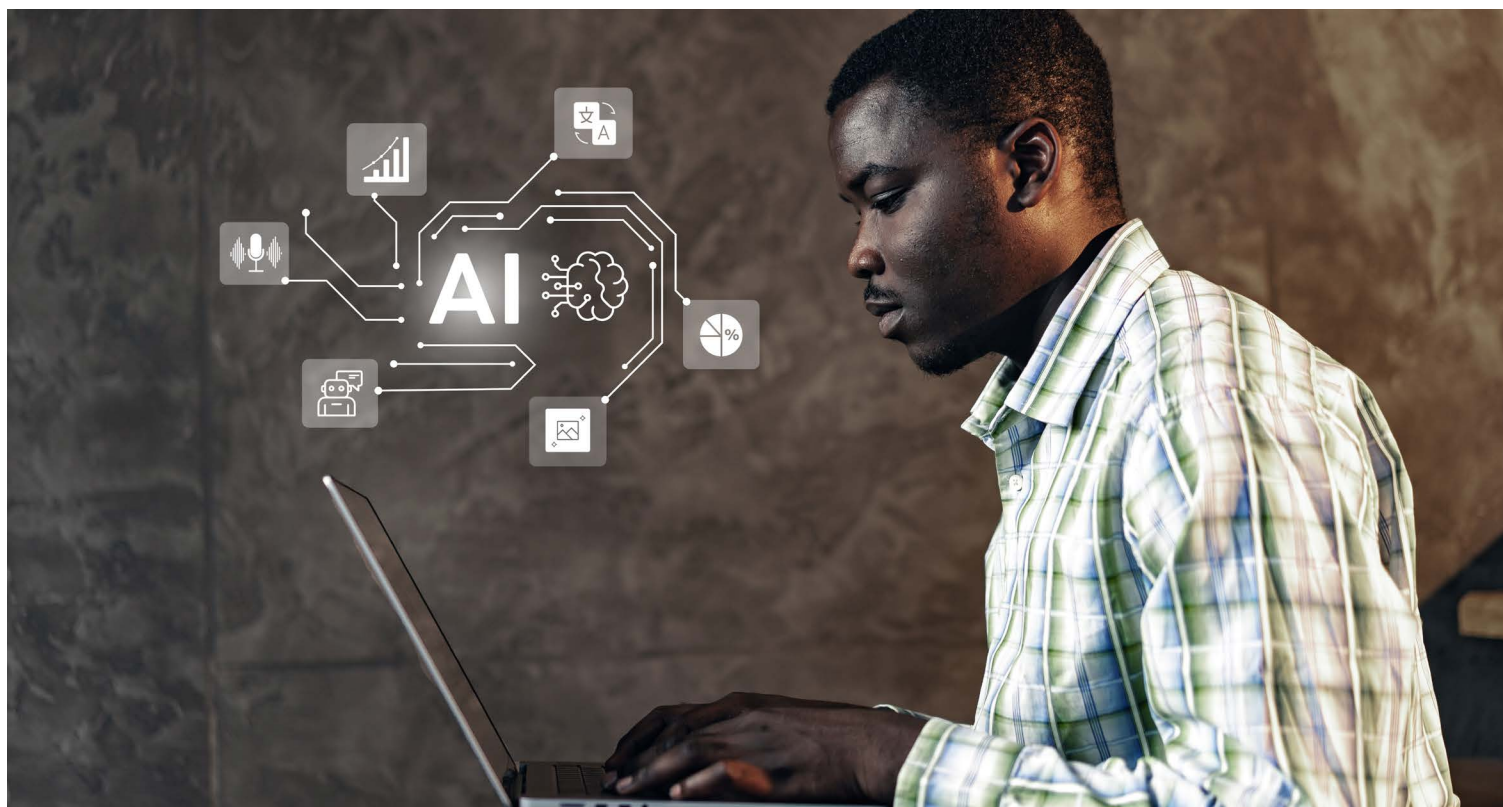
by tax authorities, business managers, *etc.*

II- The State, a promoter of AI challenged by the private sector

There can be no AI without a government policy geared towards investments that structure the digital sector. It is incumbent upon the government to lay the foundations for this technology in at least two areas.

Firstly, the State must play a key role in promoting [AI-related infrastructure](#). Beyond energy and internet connectivity infrastructure, this involves creating technology hubs, that serves as incubators where the conditions are right to foster innovation. This is the [model of the Silicon Valley](#), which has fostered the emergence of the digital giants (GAFAM). According to Seydina Ndiaye, this is a guarantee of digital sovereignty that prevents Africa from relying on solutions imposed by multinationals with enormous capital.

Secondly, the State has the responsibility to integrate training on [AI into academic and professional curricula](#). Its institutional support lies in subsidies and other incentives that promote research, development, and innovation. In this area, competition from foreign multinationals remains fierce, as they can easily lure human resources away from African States by offering more attractive salaries.



CREDIT: VECTEEZY

III- The State, a key regulator of Artificial Intelligence

To limit the risks associated with the use of AI, its developers implement security measures. However, given the risks posed by the use of AI, the State is called upon to strengthen its regulatory role.

Firstly, regulatory standards require establishing rules for the creation and use of AI. Therefore, the State can adopt protective measures for users or third parties, and define obligations, violations, and their corresponding penalties.

Secondly, the economic regulation of AI appears imperative, as its reckless use can create distortions among users. On the one hand, the State must impose transparency in the use of AI to ensure fair competition among users. On the other hand, the State must be able to define specific areas

excluded from or protected from AI, in a spirit of protectionism.

Finally, ethical regulation is what places humans at the center of AI. In this regard, the government must establish ethical frameworks for data privacy, security, transparency, and accountability in AI systems. In short, AI must support sustainable development, democracy, and human rights rather than despotism.

Conclusion

Moreover, it is clear that AI will shape State governance across all fronts. In turn, the State must be able to integrate it into its development policy to better leverage its potential. This policy must involve significant investments in infrastructure and multidimensional regulation encompassing normative, economic, and ethical dimensions.

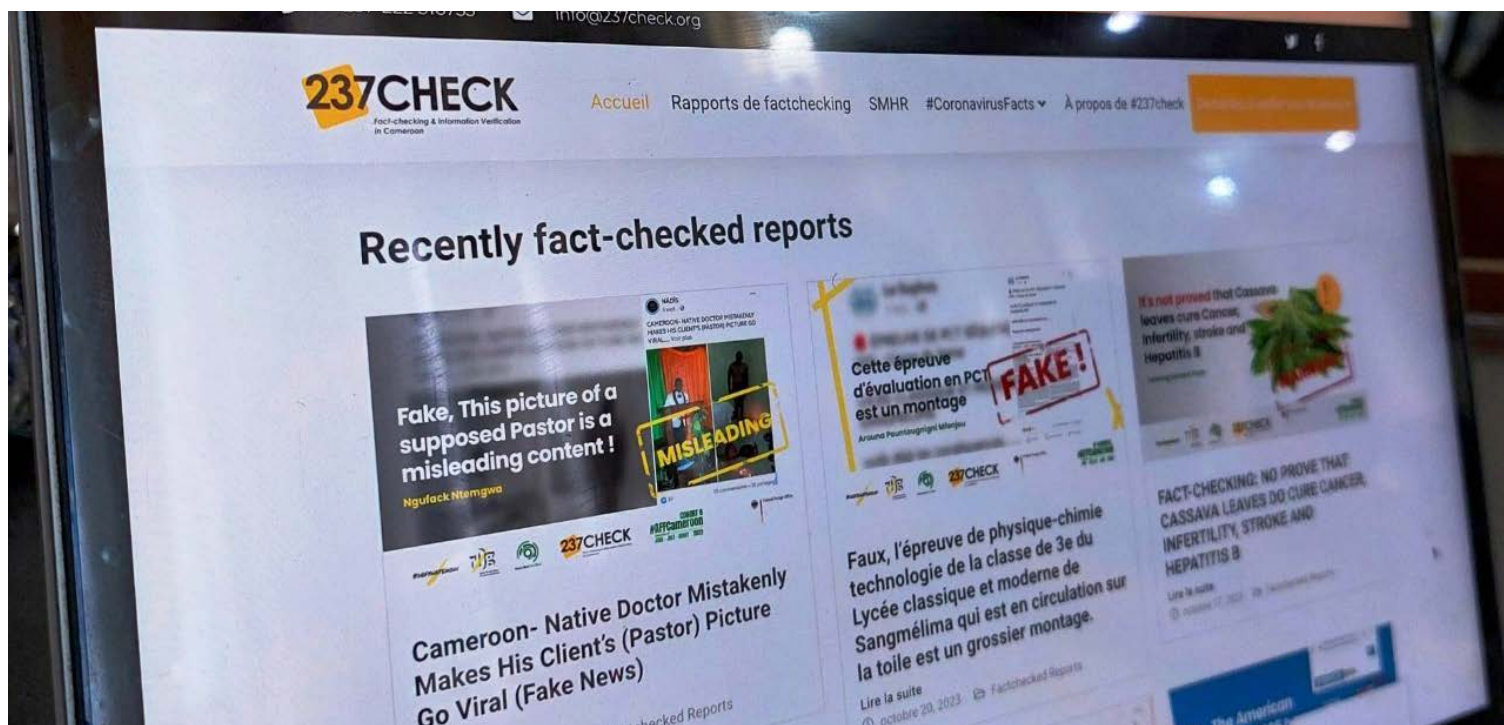
Artificial intelligence, disinformation and political (in)stability in Cameroon

In Cameroon, the rise of artificial intelligence is fueling the spread of misinformation, posing a heightened risk to political stability while underscoring the urgent need for appropriate institutional, technological, and civic responses.

By Prof. Ngo Tong Chantal

Although the practice of disinformation is as old as humanity itself, the concept is relatively recent. It first appeared in 1949 in the Dictionary of the Russian Language: *dezinformatsia*, referring to “the act of getting someone whom one wishes to mislead to accept a certain description of reality.” According to [Thierry Garcin](#), it was deployed as a weapon, a deliberate strategy implemented by the USSR to destabilize Western countries. In 1972, the English language adopted the concept of disinformation, later defined as fake news. [Fake news, or disinformation](#), was defined in 2017 by the Collins Dictionary as “false information, often sensational, disseminated under

the guise of news reporting. “The practice of fake news exacerbates social tensions and contributes to heightened uncertainty in climates of political instability. While Denis Teyssou argues that artificial intelligence is [inextricably linked](#) to the rise of deep fakes, Dimon Raymond Oyeniran maintains that AI is a significant [factor in the growth](#) of disinformation in Africa. With deep fakes, AI [serves](#) as a tool for spreading false information. The practice of editing videos that attribute statements to political figures that they did not make, known as “[deepfakes](#),” is a disinformation tool that involves manipulating videos or audio recordings using artificial



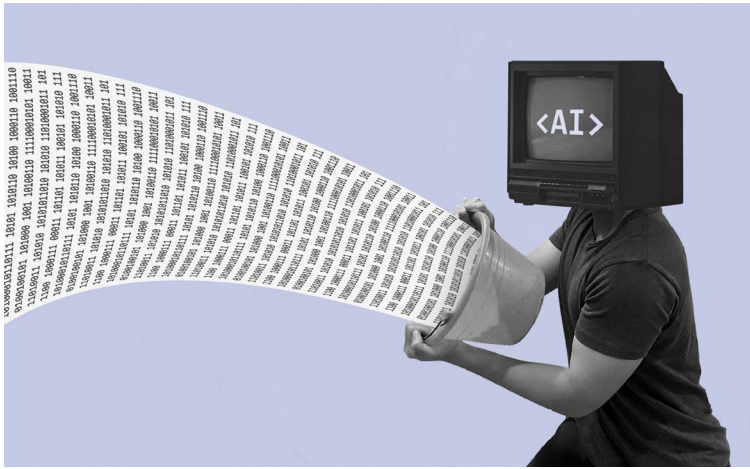
CREDIT: FACEBOOK/CIVIC WATCH CAMEROON

intelligence techniques, to make people appear to be saying or doing things they never said or did. Deepfakes-videos or audio recordings created or modified using artificial intelligence are considered as a weapon of disinformation.

According to various [Global Risks Reports, since 2024](#), disinformation has posed a serious threat to the security and stability of nations. It undermines democracy and exacerbates sociopolitical crises across African states. By fueling hate speech and polarizing public opinion on issues that incite violence, disinformation transforms information itself into a weapon against peace, security, and stability. According to the Global Peace Index (Economist Intelligence Unit), Cameroon's instability index in 2025 was 2.683 (state of peace, law), a 5-point increase, ranking 137th out of 163 countries globally. Analysts attribute much of this deterioration to disinformation. Repeated rumors about President Paul Biya's health and alleged death have destabilized the political climate, particularly during election periods. These rumors, often

amplified by manipulated images or videos, illustrate how disinformation erodes trust in institutions and heightens insecurity. It is therefore urgent to find mechanisms to assess and verify information and ensure that citizens have access to accurate information. Artificial Intelligence acts as a "double-edged sword" in this context: on the one hand, it can help detect fake news, do real-time fact-checking, and the guarantee the reliability and integrity of an information; on the other hand, it is used to create fake videos and manipulate images that constitute fake news and deepfakes.

How can political actors and civil society actors work together to mitigate the negative effects of AI and optimize its constructive potential to ensure the reliability of information, strengthen democracy, and promote healthy and constructive public debate? Collaboration and cooperation toward the common goal of building a peaceful democracy are essential in the face of the threat that disinformation poses to political stability. In a forward-looking approach combined with strategic interactionism,



CREDIT: MININX DOODLE/ISTOCK

the discussion will focus on examining, on the one hand, AI as a Tool for Disinformation and a Factor of Instability, and on the other hand, AI as an instrument of stability”.

I. AI: A tool for disinformation and a factor of instability

Disinformation, in its broadest sense, [is defined as](#)

“the manipulation of a specific target for political, military, or economic purposes, using information processed through indirect means.”

Although disinformation has long represented a global threat, its impact has reached alarming proportions in the digital age, where online platforms exponentially accelerate the spread of

false information. Disinformation disseminated through the internet, media, and social networks presents new challenges for states due to its capacity to destabilize and disrupt political order. The rise of artificial intelligence has amplified these practices. While the history of disinformation stretches back centuries, [the history of artificial intelligence](#) (AI) is more recent, dating to the post-World War II era in 1950. The term “Artificial Intelligence” appeared in 1956 to describe the ability of systems developed by computer pioneers and mathematicians to autonomously solve complex problems. Today, AI has evolved far beyond simple programming, with technologies such as Generative Adversarial Networks (GANs) enabling the creation of original, highly realistic content. In Cameroon, online rumors concerning the death or health of political figures are commonplace. For example, President Paul Biya has been the subject of death rumors on at least 39 occasions, and claims of illness or coma 13 times. Circulating in contexts of political crisis and electoral campaigns, these rumors generate insecurity and mistrust among the population. [Assiene Bissossoli and Salla Bezanga](#) analyze these rumors about the president’s death as political tools used to challenge or resist the dominant order. Such rumors, constantly disseminated, fuel hate speech, exacerbate violence, and destabilize society. In crisis situations, rumors appear as a negative phenomenon, carrying the risk of instability and destabilization of society. Furthermore, whether they concern a political figure or are used in the context of elections, rumors are a strategy for political positioning, an instrument of political competition. Philippe Aldrin speaks in this sense of [“a rumor-based approach specific to political competition and the exercise of power.”](#) Disinformation during election periods has a destabilizing effect on electoral systems and casts doubt on the credibility of the electoral process. The harmful impact of disinformation is now amplified by AI, which in 2025 was described as [“a new tool for disinformation in the presidential campaign.”](#) AI-generated images and videos were used [to persuade crowds or encourage](#)

[stances that favor](#) either the ruling party or the opposition depending on the actors involved. Thus, when deployed in schemes of manipulation, AI is a factor of instability. Yet, when harnessed for fact-checking and verification of information, AI can serve as an instrument of stability, offering tools to counter disinformation and restore trust in public discourse.

II. AI: an instrument of stability

The contribution of artificial intelligence to fact-checking makes it a significant element of socio-political stability. Fact-checking is the practice of verifying the accuracy of statements made by political leaders or other public figures. It involves examining the truthfulness of information disseminated in the media, public discourse, and on social networks. As such, it is a key tool in the fight against disinformation and fake news. The logic of fact-checking is essentially a logic of “monitoring,” ensuring that information circulating in the public sphere is reliable and trustworthy.

In Cameroon, platforms such as [#237Check](#) and [Data check](#) have been created to verify information and analyze data related to online news. These initiatives play a crucial role in countering false narratives and restoring public confidence. For example, ahead of the Pope’s upcoming visit to Cameroon from 15 – 18 April 2026, manipulated images circulated online claiming that attendees would be charged to attend Masses. Data check quickly debunked this rumor, clarifying that no fees would be imposed. This illustrates how fact-checking platforms can neutralize misinformation before it spreads widely. Similar initiatives exist across Africa. *Africa Check* in South Africa, has exposed numerous false claims relating to elections, public health, and governance. During the COVID-19 pandemic, it played a vital role in debunking myths about vaccines and treatments, thereby protecting public health.

Conclusion and recommendations

Artificial intelligence plays a dual role in a State’s socio-political landscape. On the one hand, it assists in detecting fake news, enables real-time fact-checking, and helps guarantee the reliability and integrity of information. In this way, AI contributes to improving the social climate and provides effective means of combating disinformation. On the other hand, AI is increasingly misused to create fake videos and manipulate images that constitute fake news and deepfakes. When deployed in this manner, it amplifies disinformation and becomes a destabilizing factor. For instance, in Cameroon, manipulated images have circulated during election periods, fueling rumors about political figures and undermining public trust.

In this regard, we recommend to government, enterprises and organization of civil society to:

- Develop strategies to train and strengthen the skills of fact-checkers, journalists, and civic actors to design solutions to detect fake news and ensure the reliability of information;
- Guarantee a transparent public space where reliable information can be shared within a trusted environment. Independent fact-checking platforms such as #237Check in Cameroon and Africa Check in South Africa demonstrate how civic initiatives can counter disinformation;
- Strengthening collaboration between governments, civil society, and technology companies is essential to harness AI’s constructive potential while mitigating its risks.

Ultimately, the future of democracy and stability in Africa depends on whether AI is used as a weapon of manipulation or as a tool for accountability, transparency, and peace.

Navigating Global AI Geopolitics: Africa's Role and Strategic Responses

As global AI geopolitics intensify, Africa must assert a strategic role by shaping inclusive governance frameworks, strengthening regional alliances, and leveraging its data and talent to negotiate equitable participation in the evolving digital order.

By Dr. Pippie Hughues

As artificial intelligence (AI) becomes a central driver of global economic, military, and technological power, Africa faces both unprecedented opportunities and significant challenges. The shifting geopolitical landscape around AI is dominated by [major powers](#) whose policies and technologies shape international norms and market dynamics. Artificial intelligence is reshaping global power dynamics, with leading nations using it to boost economic, security, and diplomatic influence. For Africa, AI offers opportunities for development but also risks marginalization in global technology

governance. As Africa's role in the AI geopolitical landscape is still emerging, there is a need for strategic policies to help African states navigate international AI competition, protect their interests, and leverage AI for inclusive growth by enhancing digital sovereignty, innovation, cooperation, and governance.

This policy brief examines the implications of these global AI power dynamics for African countries and proposes strategic policy responses to safeguard Africa's interests, assert agency, and foster international cooperation. Key recommendations



to address the identified problem include developing a coordinated continental AI strategy, investing in local innovation ecosystems, enhancing digital sovereignty through data governance, and engaging effectively in global AI governance forums.

Global AI Geopolitics: Power Dynamics and Trends

Artificial intelligence has emerged as a [critical domain for global power projection](#), with [major actors like the United States, China, and the European Union](#) positioning themselves as leaders in AI research, development, and deployment. While the US leverages its strong private sector, world-class research institutions, and defense capabilities to maintain AI leadership, China on its part views AI as a cornerstone of its national development and global influence ambitions. China's strategic interests center on achieving AI dominance to transform its economy, enhance social governance through AI-powered surveillance, and assert geopolitical influence through technology exports and digital infrastructure initiatives like the Digital Silk Road. AI technologies influence global power

... emerging AI research centers and innovation hubs in cities such as Nairobi, Lagos, Cape Town, and Kigali are becoming focal points for AI development and entrepreneurship within the continent.

across multiple dimensions like economic, military, and diplomatic influence. These trends illustrate how AI is not merely a technological domain but a focal point of 21st-century geopolitics.

Africa's Position in the Global AI Landscape

[AI adoption in Africa is at an early but rapidly evolving stage.](#) Various countries have started integrating AI technologies across sectors such as agriculture, healthcare, finance, and education to address pressing development needs. Examples include AI-driven mobile health applications, precision farming tools, and fintech solutions that increase financial inclusion. Several African nations have launched national AI strategies or digital transformation plans aimed at promoting AI research, innovation, and regulation. Regional bodies like the African Union are working to develop [continental frameworks to harmonize AI policies and foster collaboration](#). Additionally, emerging AI research centers and innovation hubs in cities such as Nairobi, Lagos, Cape Town, and Kigali are becoming focal points for AI development and entrepreneurship within the continent. Despite these positive developments, AI



CREDIT: NBCNEWS

research output and policy implementation remain uneven with significant variation in capacity and resources.

Risks and Opportunities for Africa

Africa's reliance on AI technologies, platforms, and expertise primarily developed and controlled by foreign powers, especially USA, China, and EU, creates vulnerabilities. This dependency can limit Africa's autonomy in shaping AI applications suited to local needs and may expose countries to geopolitical pressures or unfavorable terms of technology transfer.

The continent's vast and diverse data, from social media to health and agricultural information, is also a valuable resource. Without robust data governance frameworks, African countries risk exploitation through unauthorized data extraction, surveillance, or commercial exploitation by foreign corporations and governments, undermining privacy and

sovereignty.

Furthermore, global AI governance and standard-setting are dominated by major powers and international organizations where African voices are often underrepresented. This exclusion risks the imposition of norms, standards, and regulations that do not align with African values, priorities, or contexts, potentially marginalizing the continent in global AI governance. Increased digitalization and AI adoption exposes

African countries to cyber-attacks, information manipulation, and AI-enabled threats.

In terms of opportunities, Africa can bypass traditional development stages by adopting advanced AI technologies directly, accelerating progress in sectors such as healthcare, agriculture, education, and financial services. This leapfrogging potential allows faster achievement of development goals and improved competitiveness in the global economy.

African countries have the opportunity to influence the development of ethical AI frameworks that reflect their cultural values, social priorities, and development needs. By championing inclusive, transparent, and human-centric AI principles, Africa can contribute to a more balanced and diverse global AI governance landscape.

AI and digital technologies can drive deeper regional integration by harmonizing policies, facilitating cross-border data flows, and enabling shared infrastructure and innovation ecosystems. This integration can create larger markets, attract investment, and strengthen collective bargaining

power on the global stage.

With a young, dynamic population and growing tech ecosystems, Africa has significant potential to nurture homegrown AI talent and startups. Supporting innovation locally can reduce dependency, create jobs, and develop solutions tailored to African realities. Balancing these risks and opportunities requires coherent policies that empower African countries to protect their digital sovereignty, participate effectively in global AI governance, and leverage AI technologies for sustainable and inclusive development.

Conclusion

As artificial intelligence reshapes global power structures, Africa stands at a critical crossroad. While the continent faces significant challenges, including technological dependency, infrastructural gaps, and limited representation in global AI governance, it also possesses unique opportunities

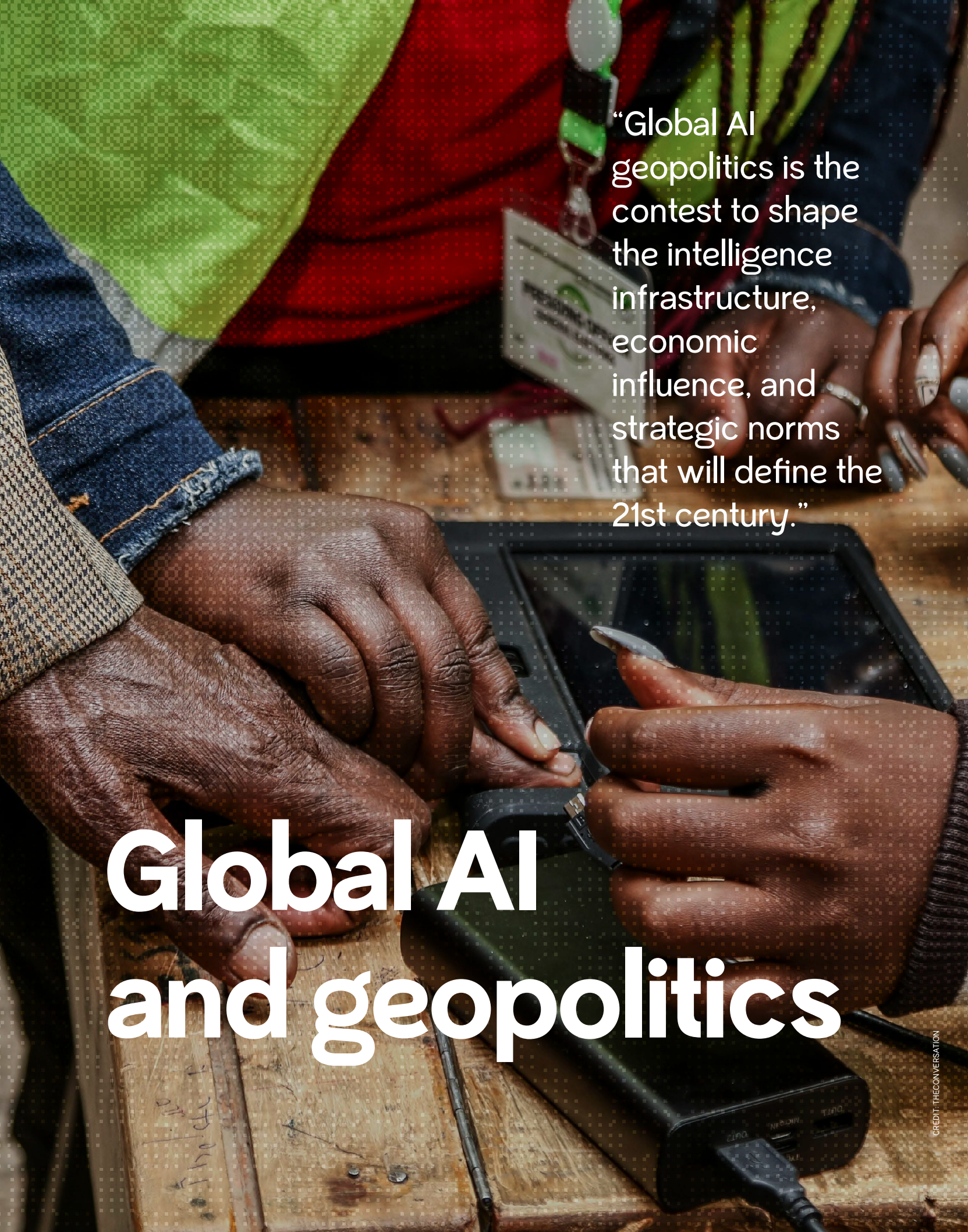
to leverage its youthful population, emerging tech ecosystems, and regional cooperation frameworks. By adopting coherent and forward-looking strategic policies that prioritize digital sovereignty, capacity building, and ethical AI development, African countries can transform these challenges into strengths. Proactive engagement in international AI dialogues and the cultivation of inclusive innovation ecosystems will enable Africa not only to safeguard its interests but also to emerge as a meaningful contributor to the global AI landscape. Ultimately, Africa's ability to navigate the complexities of global AI geopolitics will determine its role in shaping a future where technology drives sustainable development, equitable growth, and shared prosperity across the continent and beyond.

Key Policy Recommendations:

- Africa should establish a Pan-African AI Coordination Body to unify AI policies and advocate for the continent globally.
- Investments in AI education and innovation hubs are essential to foster research, support startups, and develop talent.
- Strengthening data sovereignty through robust protection laws, data localization, and improved digital infrastructure is critical.
- Active participation in international AI governance forums will help Africa influence global standards.
- Lastly, promoting ethical and inclusive AI development ensures that technological advances align with African values and benefit all communities, especially the marginalized.



CREDIT: MICROSTOCKHUB



“Global AI geopolitics is the contest to shape the intelligence infrastructure, economic influence, and strategic norms that will define the 21st century.”

Global AI and geopolitics

PEACE AND SECURITY

Digital Authoritarianism and Electoral Security in Africa:

Regulating Disinformation Without Curtailing Civic Space

Balancing electoral security and civil liberties in Africa requires nuanced regulation of digital disinformation that counters authoritarian misuse of technology while safeguarding open civic space and democratic participation.

By Enowbachem Agbortanyi

The rise of digital authoritarianism in African elections

Digital technologies have been at the heart of political mobilization, voter education, and election monitoring in Africa. However, these technologies have also introduced new possibilities for digital authoritarianism, including the use of surveillance, internet shutdowns, and restrictive legislation to control

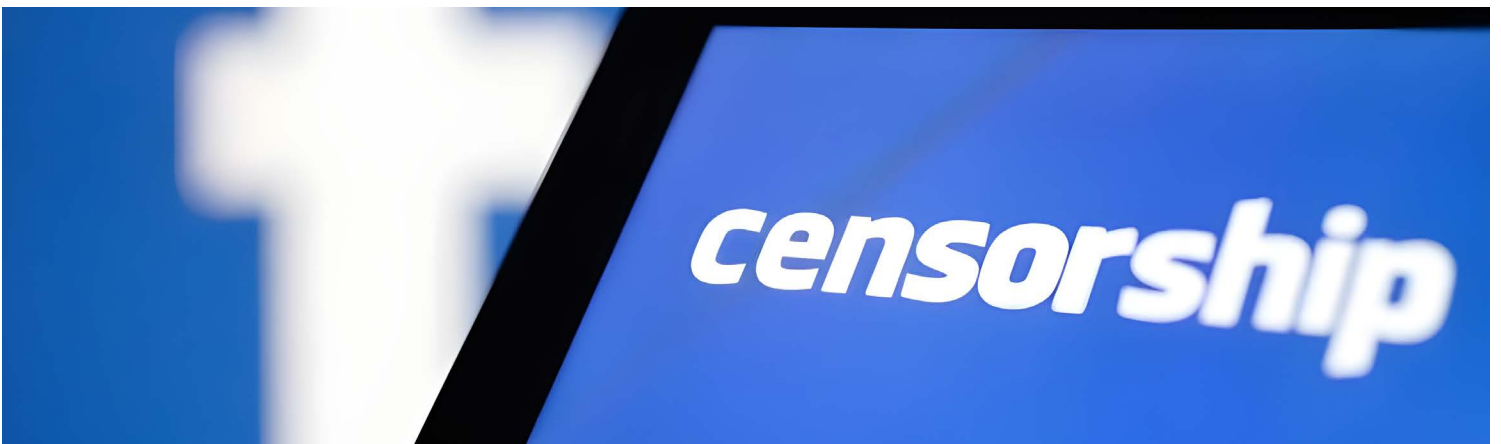
political narratives and crackdown on dissent during election times. New evidence indicates that governments across the continent are increasingly using digital infrastructure to manipulate election outcomes. [Internet shutdowns](#), content restrictions, and surveillance are often cited as measures to curb the spread of disinformation or maintain law and order. Nevertheless, these practices are often criticized for undermining the transparency of election outcomes and democratic participation.



Social media algorithms have also escalated this since they can promote content that is sensational and can create echo chambers and misinformation ecosystems.

A [report](#) by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) indicates that several countries in Africa, including Chad, Uganda, Gabon, and Zimbabwe, have been guilty of internet shutdowns during election times or protests. The cases of internet shutdowns are on the rise. For example, in [2022](#), 201 shutdowns were recorded, and the following year, there was a 41% increase to 283 internet shutdowns in 39 African countries. Internet shutdowns are often cited for undermining democratic governance and limiting the ability of citizens to communicate and participate in election monitoring. Similarly, there has been an increase in the censorship of social media and political debates during election seasons. For example, in Uganda, there was Facebook censorship as a result of accusations of interfering with domestic politics. This is an indication of the tensions between governments and digital platforms during election seasons. At the same time, there has been an escalation of digital platforms as channels for political influence operations. There are [bots and propaganda machines](#) that have polarizing effects on politics. Social media algorithms have also escalated this since they can promote content that is sensational and can create echo chambers and misinformation ecosystems.

This indicates a paradox whereby digital technologies have both positive and negative effects on democracy and election security in Africa.



CREDIT: THEREGISTER



CREDIT: FLORENT VERGNES/AFP

Disinformation, AI propaganda, and electoral instability

Disinformation campaigns are increasingly defining the nature of electoral competition in African elections. Political actors, foreign influence networks, and domestic propaganda machinery are using social media platforms to disseminate wrong information, shape public opinion, and undermine electoral processes. Evidence of several African elections shows the scope of the challenge. For instance, in [Uganda's elections](#), political actors employed hashtag campaigns, fake accounts, and misleading imagery to shape online discourse and mobilize supporters. Similarly, misinformation campaigns against opposition leaders were observed in [Angola's elections](#), showing the scope of digital propaganda in electoral processes. This is because the emergence of [generative artificial intelligence](#) (AI) has further complicated these issues. AI-generated images and propaganda materials like deepfakes have emerged as key tools for manipulating political perceptions and creating false narratives around political leaders and electoral processes. There is concern that such tools may create major disruptions in democratic processes in

many sub-Saharan African countries. In the Sahel, coordinated propaganda efforts have also leveraged manipulated imagery and viral social media content to depict political leaders as heroes or cast their opponents in a negative light, [especially in Burkina Faso](#). These propaganda efforts often leverage the disenchantment of the populace with governance and foreign interference, making them particularly effective in unstable political climates. The rising rates of digital disinformation pose significant threats to the integrity of democratic processes. Misinformation on voting processes, procedures, or allegations of electoral manipulation can erode trust in democratic processes and lead to political violence. However, overbearing government actions, such as shutting down the internet or criminalizing online free speech, tend to heighten tensions and restrict transparency and free political expression.

Policy pathways: Combating disinformation while protecting civic space

However, it is important to address the issue of digital disinformation without compromising democracy and freedoms. The following strategies



CREDIT: FRANCE24

can help African governments and regional institutions to address electoral security while promoting democracy and freedoms on the continent.

Governments must establish clear and rights-based regulatory frameworks for digital platforms. Instead of blanket censorship and shutdowns, governments must focus on well-defined regulations around coordinated disinformation campaigns, transparency in political advertisements, and algorithmic accountability. Independent regulatory bodies must be used for enforcement instead of security forces.

Governments should invest in fact-checking and digital literacy programs. Improving citizens' ability to critically analyze information online is a key component of long-term resilience against misinformation. Collaboration between electoral bodies, civil society groups, and technology firms can facilitate the design of misinformation monitoring tools

Civic space protection should be a core electoral governance tenet. Civil society organizations and digital rights advocacy play an important role in enhancing electoral transparency through citizen monitoring platforms.

Regional bodies like the African Union should also establish continental standards on digital governance in and around elections. Such standards should, for instance, prohibit internet shutdowns, enhance the transparency of

political campaigns, and foster cooperation against coordinated disinformation campaigns.

Africa's digital politics is at a critical moment in which elections are increasingly taking place in cyberspace especially with constant communications and citizens engagement throughout the process. While digital technologies hold promises for increasing electoral participation and transparency, they also carry risks of disinformation campaigns and digital repression that could undermine democratic governance. A sustainable way forward for African democracies is to balance the regulation of digital manipulation with the protection of basic freedoms that underpin democratic governance. By adopting open regulations, digital literacy, and protection of civic space, African democracies can mitigate risks of digital authoritarianism and harness digital technologies to strengthen, not undermine, electoral governance in Africa.

Optimizing Artificial Intelligence for Conflict

The case for Multilateral Cooperation and Localized

Optimizing artificial intelligence for conflict prevention in Africa requires a dual focus on multilateral cooperation and localized innovation, enabling context-sensitive early warning systems while fostering coordinated, cross-border responses to

By Anthony Antem

Artificial intelligence (AI) is rapidly emerging as a transformative tool for early warning and conflict prevention, particularly through tools such as early warning systems and predictive analytics that enhance the ability to anticipate and respond to conflict risks, thereby offering unprecedented capabilities for real-time monitoring of instability. Former U.S. President Joe Biden, in a [statement](#), further described this emerging trend as an “enormous potential and

enormous danger”. This growing relevance comes at a time when many parts of Africa continue to experience rising levels of conflict and fragility, underscoring the urgent need for more effective prevention mechanisms. While AI technologies are advancing rapidly at the global level, African countries remain largely consumers rather than creators of these systems, with limited ownership and adaptation to local contexts. A significant gap persists between globally developed AI tools and the

complex socio-political realities of African contexts, often limiting their effectiveness and relevance on the ground. At the same time, many African countries face [significant gaps](#) in data infrastructure and technical capacity, reducing their ability to develop, adapt, and effectively deploy AI systems. These limitations increase the risk of algorithmic bias, misinterpretation of conflict dynamics, and ultimately ineffective or even counterproductive predictions, undermining the potential of AI as a reliable tool for peacebuilding. Bridging this divide requires strengthened multilateral cooperation that brings together governments, international organizations, research institutions, and technology actors to co-develop solutions that are both inclusive and context-sensitive. Central to this effort is the advancement of locally grounded AI systems built on African data, knowledge, and expertise to enhance accuracy, legitimacy, and impact. This article therefore calls for coordinated global and regional action, increased investment in localized innovation, strengthened data ecosystems, and the establishment of ethical and governance frameworks to ensure AI effectively contributes to sustainable



*...AI can
support the
identi-
cation of
potential
threats
across
multiple
countries
before they
escalate into
full-scale
crises...*

peace and conflict prevention.

Artificial Intelligence and Conflict Prevention: Opportunities for Africa

Artificial intelligence (AI) offers significant opportunities for strengthening Africa's continental early warning systems (CEWS) by enhancing conflict prevention through advanced risk mapping and predictive analytics tailored to existing CEWS and Regional Economic Communities (RECs). Integrated into these mechanisms, AI can support the identification of potential threats across multiple countries before they escalate into full-scale crises, improving the timeliness and precision of alerts as highlighted in the [SIPRI Policy Report](#) on Artificial Intelligence for Climate Security. By enabling real-time monitoring of conflict indicators such as population displacement, political instability, and social tensions AI-driven systems can generate actionable insights on emerging patterns of insecurity across the continent. Within frameworks such as the African Union Peace and Security architecture, these capabilities can significantly strengthen situational awareness, enabling more informed, coordinated, and proactive decision-making by governments and regional



CREDIT: ICRC

bodies. Ultimately, the integration of AI into Africa's early warning systems can enhance the effectiveness of prevention strategies and support more timely, strategic, and harmonized peace and security responses across regions.

Challenges of Relying on Imported AI Models

The effectiveness of artificial intelligence (AI) in conflict prevention is often undermined by cultural and socio-political blind spots embedded in many existing models, which fail to fully capture the complexity of African contexts. These limitations are further exacerbated by [significant data gaps](#) and the poor representation of local realities, leading to incomplete analyses. As a result, there is a heightened risk that such systems may reinforce existing biases, misinterpret conflict dynamics, and ultimately contribute to inaccurate or misleading diagnoses of emerging crises.

The Case for Localized AI Innovation

Advancing the effectiveness of artificial intelligence (AI) for conflict prevention in Africa requires the deliberate development of African-owned datasets and locally trained models that accurately reflect the continent's diverse realities. Integrating local knowledge systems, cultural contexts, and indigenous languages into AI design further enhances the relevance and precision of these tools. Together, these efforts contribute to strengthening the legitimacy, acceptance, and trust in AI-driven interventions among communities and policymakers, thereby improving their overall impact in peace and security efforts.

Role of Multilateral Cooperation

Effective optimization of artificial intelligence (AI)

for conflict prevention in Africa requires robust coordination through regional and continental platforms such as the African Union, UN, EU etc. which can provide strategic leadership and policy coherence. This should be complemented by strengthened partnerships with global technology actors and leading research institutions to leverage expertise, innovation, and technical capacity. In addition, structured knowledge-sharing frameworks and joint funding mechanisms are essential to support collaborative research, scale successful initiatives, and ensure sustainable investment in AI-driven peace and security solutions across the continent.

Conclusion

The successful deployment of artificial intelligence (AI) for conflict prevention in Africa depends on a well-coordinated and inclusive institutional ecosystem that brings together key stakeholders at multiple levels. Governments play a central role in establishing robust policy frameworks and ensuring effective regulatory oversight, while universities and research centers drive innovation, knowledge production, and capacity building to strengthen local expertise. Regional bodies are essential for fostering coordination and operationalizing early warning systems that transcend national boundaries, and civil society organizations contribute by promoting accountability, inclusivity, and community-level engagement in AI-driven interventions. Collectively, this multi-actor framework underscores the transformative potential of AI in enhancing conflict prevention across the continent. However, its effectiveness is contingent upon strong cooperation among stakeholders and the deliberate contextualization of technologies to reflect Africa's diverse realities. Ultimately, there is a pressing need to move beyond dependency on externally developed systems toward African ownership, leadership, and innovation in AI, ensuring that the continent not only adopts but actively shapes the future of AI in global

peace and security governance.

Policy Recommendations

To effectively optimize artificial intelligence (AI) for conflict prevention in Africa, it is recommended that stakeholders:

Prioritize the development of an African-led AI strategy under the auspices of the African Union, ensuring continental coherence, local ownership, and strategic direction. This should be supported by substantial investment in localized data ecosystems and the development of African-trained AI models that accurately reflect the continent's diverse socio-political realities.

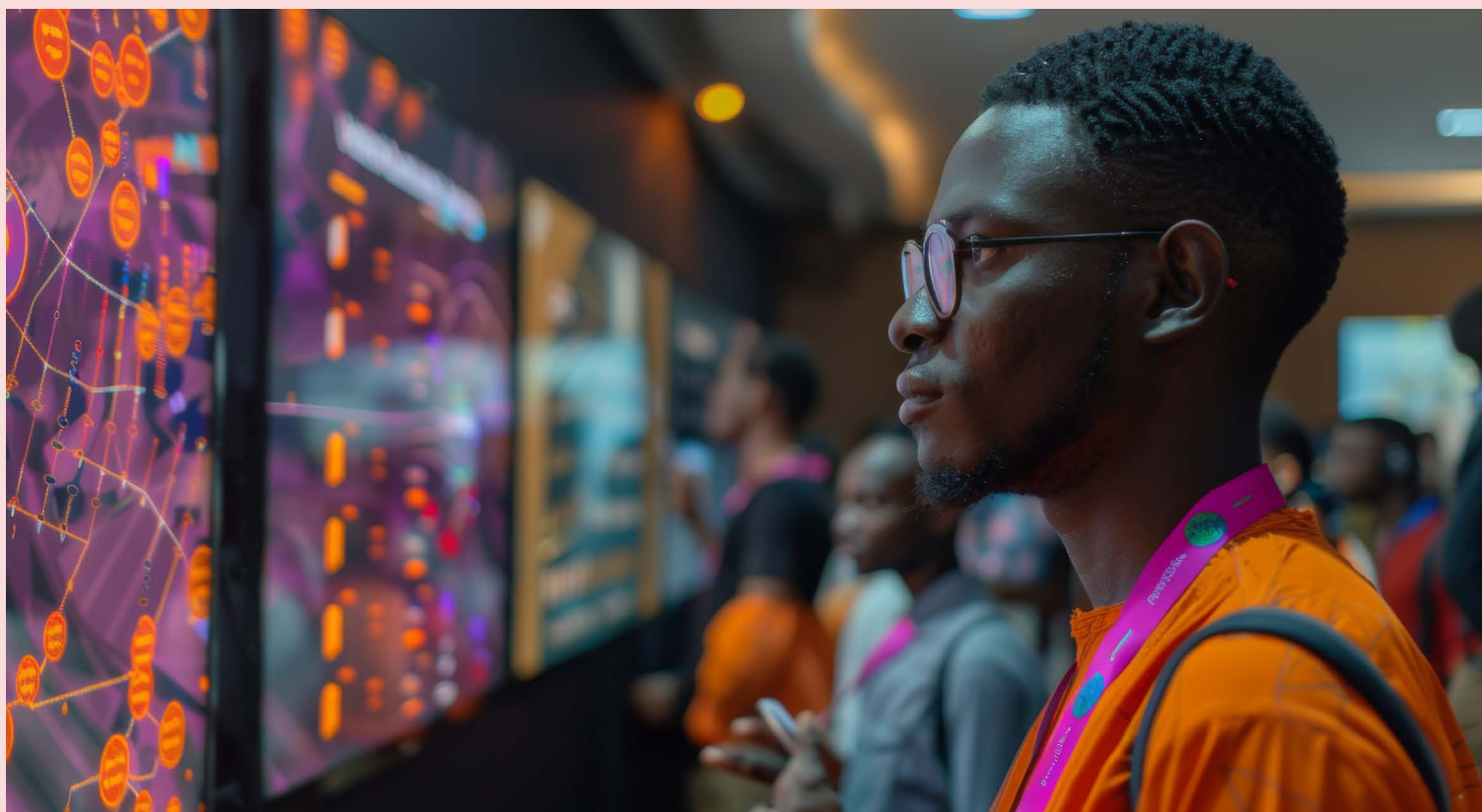
In parallel, the establishment of regional AI hubs dedicated to peace and security innovation would strengthen collaboration, knowledge exchange, and applied research, while reinforced multilateral partnerships between African institutions and global technology and research actors would enhance technical expertise and resource mobilization.

Capacity building efforts should also focus on strengthening technical skills and AI literacy across public institutions to ensure effective adoption and governance of emerging technologies. Importantly, all deployments must be guided by strong ethical standards and safeguards to mitigate risks related to bias, misuse, and unintended consequences.

However, successful implementation will require addressing key constraints, including limited financing and the need for sustainable resource mobilization, concerns over data governance and digital sovereignty, challenges related to political will and cross-border coordination, and the establishment of robust monitoring, evaluation, and adaptive learning systems to ensure continuous improvement and accountability in AI-driven peace and security initiatives.

Closing Insight

Policy Takeaways Across the Issue



CREDIT: VECTEEZY

Digital Infrastructure, Harmonized regulations and digitalization of public services

Central Africa's integration in the 21st century must move beyond physical infrastructure to prioritize digital sovereignty anchored in cloud systems, harmonized regulations,

and AI-enabled public and private services. The region risks economic marginalization if it fails to develop shared digital infrastructure, as control over data increasingly determines economic and geopolitical power in the global digital economy. A coherent policy response should therefore focus on establishing regional cloud hubs, standardizing

data, cybersecurity, and digital payment regulations, and accelerating the digitization of key public services such as customs, taxation, identity systems, and payments to generate demand for local infrastructure and attract private investment.

Integrated data systems, regulatory oversight and local computing capacity

AI regulatory sandboxes present Africa with a strategic opportunity to align rapid AI-driven health innovation with adaptive and context-sensitive governance by enabling supervised testing of emerging solutions while protecting patient rights and strengthening public trust. However, to fully realize this potential, a broader policy shift is required toward behavioral data governance that goes beyond conventional data protection frameworks to regulate algorithmic transparency, accountability, and restrictions on manipulative behavioral targeting, particularly in sensitive sectors such as digital finance where AI increasingly shapes user decisions. This must be complemented by urgent investment in interdisciplinary research capacity at the intersection of neuroscience, behavioral economics, and AI to strengthen Africa's ability to understand and govern the cognitive impacts of digital systems, thereby enabling evidence-based policymaking rooted in local expertise.

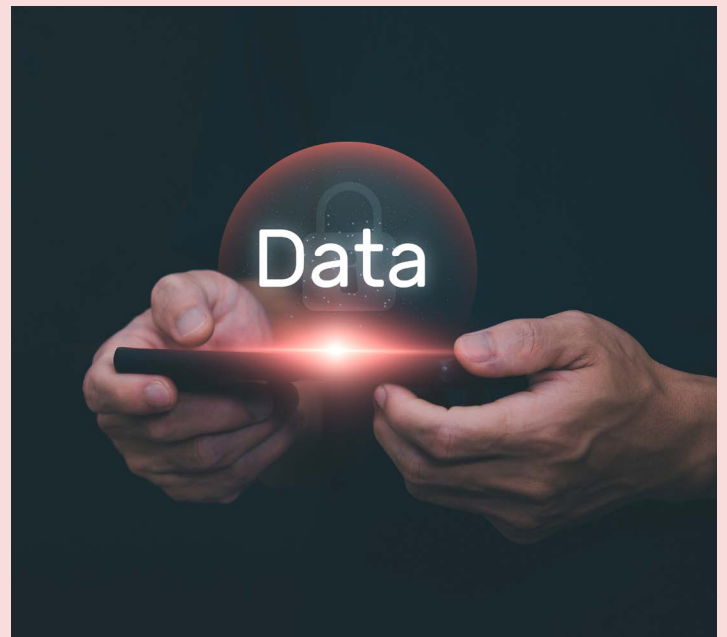
Create AI Hubs and Startups, Enhance Multidimensional coordination of AI

Artificial intelligence (AI) is emerging as a central factor in state governance and development in Africa, but its impact is twofold: it can both enhance the reliability of information by detecting fake news and deepfakes, and, conversely, be used to produce manipulative content that destabilizes societies. To fully leverage its benefits while minimizing its risks, Africa must adopt an integrated strategy combining investments in digital infrastructure, strengthening

the skills of fact-checkers, and multidimensional regulation normative, economic, and ethical. This approach should include the creation of a Pan-African Coordination Body for AI to harmonize policies across the continent and defend African interests in international forums.

Continental-wide Coordination of AI for Conflict Prevention in Africa

To effectively optimize artificial intelligence (AI) for conflict prevention in Africa, a coordinated and African-led approach under the auspices of the African Union is essential to ensure continental coherence, local ownership, and strategic direction, supported by sustained investment in localized data ecosystems and African-trained AI models that reflect the continent's diverse socio-political realities. This should be complemented by the establishment of regional AI hubs focused on peace and security innovation to strengthen collaboration, knowledge exchange, and applied research, alongside reinforced multilateral partnerships between African institutions and global technology and research actors to enhance technical capacity and resource mobilization.

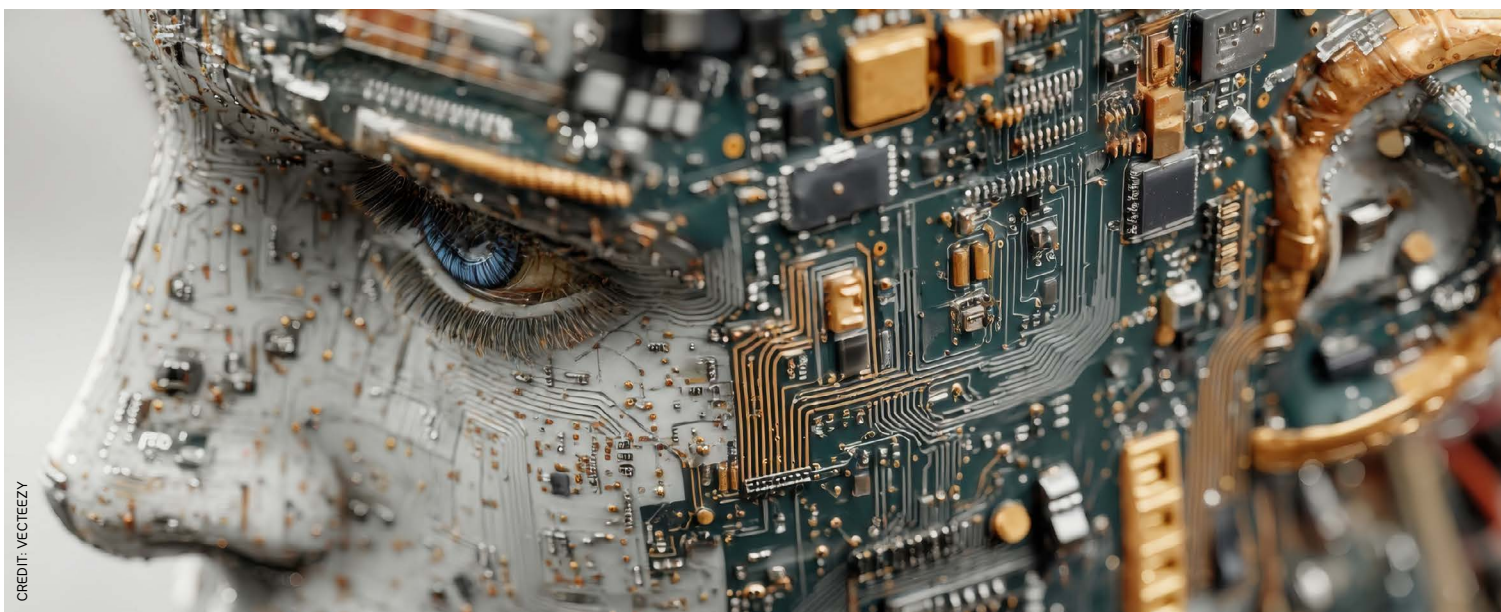


CREDIT: VECTEEZY

Final Note

This thirty first issue of *On Policy Magazine* demonstrates that Africa's engagement with the AI revolution is ultimately a question of sovereignty, agency, and strategic positioning in a rapidly shifting global digital order. Digital sovereignty is no longer a theoretical aspiration but a practical necessity for safeguarding data, shaping innovation pathways, and ensuring that technological transformation aligns with the continent's development priorities. While artificial intelligence presents immense opportunities for economic growth, service delivery, governance efficiency, and conflict prevention, it also introduces new vulnerabilities linked to data extraction, algorithmic dependency, and external technological

control. Africa's response must therefore be both ambitious and coordinated, grounded in strong institutions, harmonized regulatory frameworks, and sustained investment in digital infrastructure and human capital. By strengthening continental cooperation, fostering ethical and inclusive AI ecosystems, and asserting greater control over data and computational resources, Africa can move from being a passive consumer of technologies to an active architect of the global AI future. Ultimately, the choices made today will determine whether the continent merely adapts to the AI revolution or decisively shapes it in line with its own values, interests, and long-term development vision.



CREDIT: VECTEEZY

“Africa's response must therefore be both ambitious and coordinated, grounded in strong institutions, harmonized regulatory frameworks, and sustained investment in digital infrastructure and human capital.”



OP

Africa and AI...

www.onpolicy.org