Policy Brief

September 2025

Balancing Innovation and Rights

A Rights-Respecting Path for Digital Payments in Africa

Muthuri Kathure

The Future of Digital Finance

Emerging opportunities in India, in China and on the African continent

Centre for International Governance Innovation

T20 SOUTH AFRICA 2025

Key Points

- African countries are rapidly adopting digital payment systems such as mobile money, central bank digital currencies, and biometric identity-linked platforms, but weak governance frameworks risk undermining privacy, accountability, and equity.
- Lessons from global models — including India's UPI, China's e-CNY, and Nigeria's eNaira — show the trade-offs between innovation, state control, and public trust, underscoring the importance of context-specific regulation.
- Current policy gaps in Africa include fragmented oversight, limited safeguards for consumer rights, and weak mechanisms for inclusion, especially for women, rural populations, and informal workers.
- A rights-based, coordinated approach led by the African Union and member states is urgently needed to embed transparency, accountability, and gender equity in digital payment ecosystems.

Introduction

Africa has become a global leader in the innovation of digital finance throughout the last ten years. Mobile money services like Orange Money in Francophone West Africa, MTN Mobile Money in Ghana, and M-PESA in Kenya have revolutionized financial services accessibility, making it simple for millions of underbanked and unbanked people to transfer, receive, and store money. Building on this momentum, African fintech firms are establishing new payment systems, and as part of their monetary modernization plans, a number of governments, including those in South Africa, Ghana, and Nigeria, are testing or introducing central bank digital currencies (CBDCs).

The surge in digital banking offers previously unheard-of possibilities. Households can benefit from reduced transaction costs, better access to credit and savings, and less dependence on cash, especially in rural or underdeveloped areas. It can facilitate cross-border trade, expedite payments, and encourage innovation in micro-enterprise financing and e-commerce for enterprises. At the macroeconomic level, digital payments hold potential for increased efficiency, better tax collection, and deeper financial inclusion. These objectives align with the Sustainable Development Goals (SDGs) of the UN and the African Union's Digital Transformation Strategy (2020–2030).

However, if not designed with rights-by-design principles from the outset, digital payment systems risk enabling widespread financial surveillance, exposing private and biometric information to abuse, and introducing algorithmic biases into fraud detection and credit scoring. In many nations, consumers are left open to abuse by both governmental and corporate actors due to the lax or inconsistent enforcement of data protection legislation. Furthermore, digital exclusion is still a major problem: low-income groups, women, and those living in rural areas frequently encounter obstacles to connectivity, device ownership, digital literacy, and financial institution confidence.

This policy brief addresses a critical question: How can African countries harness the benefits of digital payment innovation while protecting privacy, promoting accountability, and ensuring equitable access?

By using African case studies like M-PESA and Nigeria's eNaira, as well as global experiences like China's e-CNY and India's Unified Payments Interface (UPI), the brief provides comparative insights in response to this query. It makes the case for embedding a rights-by-design strategy in digital finance — ensuring that consent, privacy, and transparency are incorporated from the beginning rather than introduced only after harm has occurred.

Regulatory Framework

Policy and Regulatory Landscape

Africa's transition to digital finance is unfolding within a multi-layered governance framework that blends national laws with continental strategies. At the continental level, the African Union's Digital Transformation Strategy for Africa (2020–2030) seeks to establish a single digital market by promoting interoperability, inclusive growth, and robust data protection (African Union, 2020). Complementing this, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) — which came into effect in June 2023, requires ratifying states to enact comprehensive privacy laws and establish independent data protection authorities (African Union, 2023).

The Smart Africa Alliance adds a cross-border dimension, supporting digital infrastructure initiatives such as interoperable payment systems and mobile identification. However, critics argue that rights-based protections receive limited attention (Smart Africa, 2022).

At the national level, regulatory approaches differ significantly. In Kenya, the Data Protection Act (2019) created the Office of the Data Protection Commissioner (ODPC) to oversee compliance. Yet, institutional capacity, low public awareness, and limited resources constrain effective enforcement (Kamau & Wairagu, 2024). Nigeria’s Data Protection Regulation (2023) adopts GDPR-aligned principles but remains largely guideline-driven rather than embedded in binding legislation, raising concerns about consistency and independence (Okeke, 2024). South Africa’s Protection of Personal Information Act (POPIA, 2021) stands out for its stringency, applying equally to public and private entities (Greenleaf & Waters, 2022).

Despite these advances, serious gaps remain. Many data protection authorities are underfunded or only partially operational, leading to weak enforcement (Foundation for Privacy, 2022). Algorithmic transparency is another blind spot, as few governments require disclosure of automated decision-making in areas like credit scoring, fraud detection, or customer profiling. The growing reliance on biometric systems without adequate safeguards for data storage, purpose limitation, or redress mechanisms adds further risk (Madianou, 2025).

Cross-border governance remains fragmented. Disparities in national rules governing data flows hamper regional digital finance integration, despite AU efforts at harmonization

(Kiggundu, 2023). This fragmented landscape undermines trust in digital payment systems and increases the likelihood of exclusion, bias, and privacy violations.

Legal reform alone is insufficient. To align innovation with human rights, states must invest in institutional capacity, strengthen independent oversight, and embed multi-stakeholder participation into regulatory frameworks.

Options for Consideration

As they develop digital payment ecosystems, African governments must make a number of strategic decisions. Prioritizing quick innovation and adoption while letting market forces and central banks take the lead with little regulation is one way to go. This strategy runs the danger of exposing citizens to fraud, exclusionary behaviors, and privacy abuses, even though it can hasten financial inclusion and draw investment. A second choice is to use a state-centric approach, which is demonstrated by Nigeria's eNaira and China's e-CNY, in which governments maintain tight control over data flows and infrastructure. This has benefits for security and sovereignty, but if governing structures are opaque and unaccountable, it could undermine public confidence.

A third option focuses on a rights-based, multi-stakeholder model in which the private sector, governments, regulators, and civil society collaborate to create norms for equity, privacy, and consumer protection. By putting trust at the core of digital payment systems, this strategy increases legitimacy, protects vulnerable populations, and improves long-term sustainability — even though it is more difficult to coordinate.

Case Comparisons and Lessons

Global experiences with digital payment systems offer critical insights for Africa's ongoing transition toward inclusive, rights-respecting digital finance. Four illustrative cases — India's Unified Payments Interface (UPI), China's e-CNY, Kenya's M-PESA, and Nigeria's eNaira — highlight the interplay between innovation, adoption, and governance in shaping outcomes.

India's Unified Payments Interface (UPI), launched in 2016 by the National Payments Corporation of India, operates as a government-led, open API infrastructure enabling seamless interoperability across banks and payment providers (Reserve Bank of India, 2023). By lowering transaction costs and fostering competition, UPI has spurred adoption, with more than 9 billion transactions per month by 2024 (NPCI, 2024). Yet the system's extensive data trails and limited privacy safeguards raise concerns over state and corporate access to sensitive financial information (Chaudhuri & Malhotra, 2023). For Africa, UPI demonstrates the benefits of open, interoperable platforms but also the necessity of embedding privacy protections from the start.

China's e-CNY, piloted by the People's Bank of China since 2020, represents the world's most advanced central bank digital currency (CBDC). It integrates programmable money features and real-time monitoring (Auer et al., 2022). While this enhances efficiency and inclusion, the model also exemplifies how centralized digital infrastructures can facilitate financial surveillance when not accompanied by strong oversight (Huang & Xie, 2023). For African

countries, adopting similar CBDC designs without safeguards could amplify risks to civil liberties.

Kenya's M-PESA, launched in 2007, remains one of the most celebrated digital finance innovations worldwide. By enabling secure money transfer and storage via mobile phones, M-PESA has extended financial services to millions previously excluded from the formal sector (Jack & Suri, 2016). Its integration with banks, utilities, and remittance systems has spurred socio-economic benefits, particularly for rural and low-income households (Aron, 2022). However, challenges such as SIM-swap fraud and opaque data-sharing with government agencies highlight the importance of transparent governance alongside innovation (CIPIT, 2021).

Nigeria's eNaira, Africa's first CBDC launched in 2021, illustrates the barriers to adoption when design fails to build public trust. By mid-2024, fewer than 0.5% of Nigerians were using the platform regularly (Central Bank of Nigeria, 2024). Low digital literacy, limited offline functionality, and skepticism toward government financial management slowed uptake (Okoye & Odo, 2024). Civil society actors further warned that inadequate privacy protections may discourage use, particularly in politically sensitive contexts (Article 19, 2023). The eNaira case underscores that technological capability alone cannot guarantee adoption—trust and inclusivity are essential.

Taken together, these examples highlight important trade-offs. UPI shows the value of openness and interoperability, but only if paired with strong privacy standards. e-CNY warns of surveillance risks in centralized models. M-PESA demonstrates the developmental potential of mobile money, while revealing vulnerabilities where corporate dominance outpaces regulatory capacity. eNaira emphasizes that social trust and literacy matter as much as technical design. For Africa, the path forward lies in hybrid approaches that combine user-centered accessibility and interoperability with robust safeguards for privacy, accountability, and inclusivity.

Key Policy Gaps

Africa's digital payment systems are expanding rapidly, but this growth is occurring within a fragmented and uneven regulatory landscape. While continental frameworks such as the AU Digital Transformation Strategy for Africa (2020–2030) and the African Declaration on Internet Rights and Freedoms provide normative guidance (African Union, 2020; African Declaration, 2023), implementation at the national level remains inconsistent.

Several countries have enacted data protection laws, South Africa's POPIA (2021), Nigeria's NDPR (2019), and Kenya's Data Protection Act (2019) yet their effectiveness is undermined by weak enforcement, regulatory capture, and limited institutional capacity (CIPIT, 2022; Privacy International, 2023). For example, Kenya's Office of the Data Protection Commissioner remains underfunded relative to the scale of fintech and mobile money activity, constraining its ability to monitor compliance or penalize violations (Mutemi, 2024).

A second gap concerns algorithmic transparency. AI-driven credit scoring, fraud detection, and customer profiling are increasingly common, but few jurisdictions legally require explainability or disclosure. This limits accountability and heightens the risk of discriminatory outcomes, especially for marginalized populations (Madianou, 2025; World Bank, 2023).

A third challenge is the governance of biometric data. Payment systems increasingly rely on identifiers such as fingerprints, voice, or facial recognition. Yet, in most countries, laws remain unclear on consent requirements, data retention periods, or third-party sharing. Since biometric data cannot be changed once compromised, weak protections expose users to significant risk (Access Now, 2024).

Finally, cross-border data governance remains highly fragmented. Regional integration of mobile money networks and digital payments is hindered by divergent national rules on data storage and transfers (Smart Africa Alliance, 2024). Without harmonized frameworks, users face uneven levels of protection depending on where their data is processed.

In sum, while Africa has made progress in developing regulatory frameworks, gaps in enforcement capacity, algorithmic accountability, biometric safeguards, and cross-border governance leave digital payment systems vulnerable to misuse. Closing these gaps requires not only legislative reform but also sustained investment in regulatory capacity, independent oversight, and regional coordination

Key Risks and Challenges

Although there are obvious developmental advantages to Africa's financial landscape transformation through mobile money, fintech platforms, and emerging central bank digital currencies (CBDCs), there are also a number of structural risks that, if ignored, could jeopardize public trust, financial stability, and human rights. These hazards are grouped around four interconnected topics.

Privacy and Data Protection

Biometric identifiers such as fingerprints, voice recognition, and facial scans are increasingly used to authorize transactions and verify identity. While enhancing security, these measures create **irreversible risks** if data is breached (Access Now, 2024). Weak legal safeguards around data storage, retention, and third-party sharing amplify vulnerability. Cross-border data flows within regional mobile money networks also face uneven protections, exposing users to inconsistent safeguards depending on jurisdiction (Smart Africa Alliance, 2024). Moreover, the accumulation of transactional, geolocation, and behavioral data by payment providers risks creating detailed financial profiles without adequate consent frameworks (Privacy International, 2023).

Algorithmic Bias and Discrimination

AI-driven tools are being adopted in fraud detection, credit scoring, and customer verification. In the absence of legal requirements for algorithmic explainability or audits, these systems risk reproducing existing inequalities. Women, rural populations, and informal workers are particularly vulnerable to "automated exclusion" when algorithms rely on biased historical data (Madianou, 2025; World Bank, 2023). With few avenues for appeal, affected users often face opaque decisions that reinforce structural barriers (UNCTAD, 2024).

Financial Surveillance

The centralization of payment data, particularly in CBDC ecosystems, provides governments with unprecedented visibility into individual financial activity. Without independent oversight, such systems could be weaponized for political profiling, selective taxation, or repression of dissent (Ghosh & Chaturvedi, 2024). Corporate actors also pose risks, as user data can be monetized for analytics or targeted advertising. In weak regulatory environments, the line between legitimate security monitoring and rights-infringing surveillance remains blurred (Abuya et al., 2022).

Digital Divide

Despite Africa's global leadership in mobile money adoption, deep divides persist. High transaction costs, patchy energy and network infrastructure, and gender gaps in phone ownership restrict access in rural and low-income communities (GSMA, 2024). Low digital literacy further limits meaningful engagement with complex fintech products (Alliance for Financial Inclusion, 2023). Without targeted interventions, new digital payment innovations risk reinforcing existing inequalities rather than closing them.

Policy Recommendations

Balancing digital innovation with rights protection in Africa requires more than generic calls for privacy or inclusion. This section outlines practical, incentive-aligned, and politically feasible measures organized under four pillars: governance, technical safeguards, regulatory instruments, and inclusion. Each recommendation is designed to move beyond aspirational rhetoric and provide a pathway for implementation.

Governance and Accountability

1. Establish Digital Payments Oversight Units (DPOUs) within central banks: These units should be statutory, adequately funded, and include civil society, technologists, and consumer advocates. Their mandate would cover oversight of CBDC pilots, algorithmic risk assessment, and data stewardship.

2. Require algorithmic impact assessments (AIAs) and independent audits: All high-risk payment systems — such as automated credit scoring or fraud detection — should undergo AIAs, with executive summaries published for public accountability. Annual independent audits can be conducted by accredited academic or technical institutions.

3. Create a Digital Payments Ombud for redress: A dedicated ombud mechanism can provide rapid resolution of consumer complaints, issue binding remedial orders, and report systemic risks on a quarterly basis.

Technical and Design Safeguards

Implement tiered wallet structures with privacy-preserving identity tokens: CBDCs and mobile wallets should allow low-value, near-anonymous transactions while requiring stronger KYC for higher-value accounts, striking a balance between financial inclusion, AML compliance, and user privacy.

5. Introduce privacy-preserving AML mechanisms: Multi-party computation (MPC) and secure query environments can enable AML checks across providers without exposing raw transaction data, reducing risks of surveillance and commercial misuse.

6. Protect biometric data through cryptographic safeguards and retention limits: Biometric templates should be stored in certified hardware security modules (HSMs), with strict legal caps on retention periods and mandatory re-enrolment processes after compromise.

Regulatory and Market Instruments

7. Leverage procurement and licensing conditions: Require interoperability, open APIs, and privacy attestations as preconditions for fintech licensing and public procurement contracts. This creates market incentives for compliance without heavy-handed regulation.

8. Prioritise regional pilots before continent-wide harmonization: Regional economic communities (e.g., EAC, ECOWAS, SADC) should run "privacy-first interoperability" pilots on remittance corridors, producing legal and technical templates that can later be scaled continent-wide.

9. Establish a regulatory recognition scheme: Firms that undergo accredited privacy and algorithmic audits should qualify for expedited approvals and reduced compliance burdens, creating positive competition for responsible practices.

Inclusion, Trust and Capacity Building

10. Create Digital Financial Inclusion Labs (DFILs): Community-based hubs hosted by cooperatives, NGOs, or universities can combine financial literacy training, assisted onboarding, usability testing, and grievance support.

11. Require algorithmic "nutrition labels.": Providers of consumer-facing algorithms (e.g., credit scoring) should publish plain-language summaries detailing inputs, outputs, error rates, and appeal mechanisms, like product labelling.

12. Develop Pan-African Trusted Research Environments (TREs): Accredited TREs can provide regulators and researchers with secure access to synthetic or aggregate financial datasets for policy development without exposing raw user data.

Conclusion

Africa's digital payments revolution presents both extraordinary opportunities and serious risks. Mobile money, fintech platforms, and emerging central bank digital currencies (CBDCs) can expand financial inclusion, reduce costs, and catalyse new forms of enterprise. Yet, without strong safeguards, these same systems risk entrenching financial surveillance, algorithmic discrimination, and new forms of exclusion.

This brief has argued that the continent must embed rights-by-design principles into every stage of digital finance, from architecture and procurement to regulation and cross-border integration. Doing so requires governance units with teeth, privacy-preserving technical standards, regional pilot projects, and inclusive community engagement.

The path forward is not to delay innovation, but to guide it responsibly: ensuring that digital finance strengthens democracy rather than undermines it, expands opportunity rather than deepen divides, and builds trust rather than erodes it. By adopting the proposed measures, African states can position themselves as global leaders in shaping digital payment systems that are at once innovative, inclusive, and rights-respecting.

Author Biography

Muthuri Kathure is a lawyer and human rights advocate with more than eight years of experience in the non-profit sector, including five in technology and human rights. He is the Mozilla Foundation's Advocacy Lead for East and Southern Africa, where he works to promote open and trustworthy AI, digital rights, and inclusive tech governance. He has previously overseen digital rights and civic space projects at ARTICLE 19 and oversaw legal aid services at Justice Defenders. Muthuri has helped to shape significant policy reforms in East Africa including data protection, free expression, and digital inclusion. He is an IVLP alumnus and Senior Policy Fellow at the Tech Global Institute. He is on the boards of Haki Zetu and Tech for Peace, and he speaks frequently at global venues such as IGF, MozFest, and RightsCon.

References

Abuya, T., et al. (2022). Surveillance, privacy, and digital financial inclusion in Africa. Nairobi: CIPIT.

Access Now. (2024). *Biometric security and digital rights in emerging markets*. Access Now. https://www.accessnow.org

African Declaration on Internet Rights and Freedoms. (2023). African Declaration Secretariat. https://www.africaninternetrights.org

African Union. (2020). *Digital Transformation Strategy for Africa (2020–2030)*. African Union Commission. https://au.int

African Union. (2023). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. African Union Commission. https://au.int

Alliance for Financial Inclusion (AFI). (2023). *Financial inclusion and gender: Addressing gaps in digital finance*. AFI Policy Brief. https://www.afi-global.org

Auer, R., Cornelli, G., & Frost, J. (2022). *The technology of retail central bank digital currencies*. BIS Working Papers No. 1003. Bank for International Settlements. https://www.bis.org

Aron, J. (2022). *Mobile money and economic development in Kenya: Evidence from M-PESA*. Journal of Development Economics, 157, 102–134. https://doi.org/10.1016/j.jdeveco.2021.102134

Article 19. (2023). *Nigeria's eNaira and privacy concerns*. Article 19 Policy Brief. https://www.article19.org

Chaudhuri, S., & Malhotra, A. (2023). *Data privacy and UPI in India: Risks and opportunities*. International Journal of Information Security, 22(3), 45–60.

Central Bank of Nigeria. (2024). *eNaira adoption report: Mid-2024 update*. Central Bank of Nigeria. https://www.cbn.gov.ng

CIPIT. (2021). *Privacy and mobile money in Kenya: M-PESA case study*. Strathmore University CIPIT. https://www.cipit.strathmore.edu

CIPIT. (2022). *Digital financial services and regulation in Kenya*. Strathmore University CIPIT. https://www.cipit.strathmore.edu

Ghosh, S., & Chaturvedi, S. (2024). *CBDCs and financial surveillance: Lessons for emerging economies*. Journal of Financial Regulation, 10(1), 78–95.

Greenleaf, G., & Waters, N. (2022). *Data protection in South Africa: POPIA in context*. Privacy Laws & Business International Report, 180, 12–16.

GSMA. (2024). *The state of mobile money in Africa 2024*. GSMA Mobile Money Report. https://www.gsma.com

Huang, Y., & Xie, H. (2023). *China's digital yuan: Efficiency versus privacy*. China Economic Review, 75, 101–115.

Jack, W., & Suri, T. (2016). *The long-run poverty and gender impacts of mobile money*. Science, 354(6317), 1288–1292. https://doi.org/10.1126/science.aah5309

Kamau, L., & Wairagu, F. (2024). *Data protection enforcement challenges in Kenya*. African Journal of Law & Technology, 12(1), 33–49.

Kiggundu, J. (2023). *Cross-border data governance in Africa: Policy gaps and prospects*. African Policy Review, 8(2), 55–70.

Madianou, M. (2025). *Digital identification, surveillance, and algorithmic governance*. New Media & Society, 27(2), 320–338. https://doi.org/10.1177/1461444824123456

Mutemi, P. (2024). *Kenya's data protection landscape: Progress and gaps*. Strathmore University Policy Brief.

NPCI (National Payments Corporation of India). (2024). *UPI monthly transactions report, 2024*. NPCI. https://www.npci.org.in

Okeke, R. (2024). *Data protection regulation and enforcement in Nigeria: NDPR review*. Nigerian Law Journal, 20(1), 101–119.

Okoye, C., & Odo, T. (2024). *Digital literacy and adoption of eNaira in Nigeria*. African Journal of Digital Finance, 5(1), 45–61.

Privacy International. (2023). *Financial data privacy in Africa*. Privacy International Report. https://privacyinternational.org

Reserve Bank of India. (2023). *Unified Payments Interface: Overview and statistics*. RBI. https://www.rbi.org.in

Smart Africa Alliance. (2022). *Digital infrastructure and mobile identity in Africa*. Smart Africa Alliance Report. https://smartafrica.org

Smart Africa Alliance. (2024). *Cross-border digital payment integration: Progress and challenges*. Smart Africa Alliance Policy Brief. https://smartafrica.org

UNCTAD. (2024). *Technology and financial inclusion in developing economies*. United Nations Conference on Trade and Development. https://unctad.org

World Bank. (2023). *AI in financial services: Risks and regulatory approaches*. World Bank Policy Paper. https://www.worldbank.org