

Policy Brief

Governing Digital Public Infrastructure for Rights & Equity in Africa





POLLICY

Authors: Bonaventure Saturday and Bobina Zulfa

Reviewers: Neema Iyer, Bonnita Nyamwire, Adebayo Odunlami and Angela Minayo

Suggested Citation:

Saturday, B., and Zulfa B., (2025). Governing Digital Public Infrastructure for Rights and Equity in Africa. Policy Brief.

January 2026

Background

Digital Public Infrastructure (DPI), which includes digital identification systems, mobile payments, and data-sharing platforms, has become central to Africa's digital transformation agenda. Although DPI is frequently framed as a means of improving efficiency and expanding access to essential services, its current implementation across the continent reveals a widening disconnect between technological ambition and social reality. Women, ethnic minorities, gender-diverse communities, and other underrepresented groups often experience DPI not as an enabler of inclusion, but as an additional barrier to participation. This policy brief argues that rights-respecting and equity-focused governance is essential if DPI is to advance, rather than undermine, social justice.

While DPI promises streamlined services, its rollout commonly reflects state-centred priorities such as administrative control, revenue collection, or institutional efficiency, more than the everyday needs of citizens. Many systems are introduced with limited consultation, little attention to context, and minimal engagement with the communities most affected by the transition to digital systems. This approach sits uneasily within societies where long-standing gendered and structural inequalities shape access to devices, connectivity, mobility, and digital skills. When DPI is layered onto these uneven foundations, it risks amplifying existing divides. In many cases, accessibility features are added only after deployment, and the rationale for new systems remains opaque, generating confusion and public mistrust.

Key Findings

The Digital Public Infrastructure Governance Crisis: Exclusion by Power and Practice

DPI broadly defined in this study's literature review can be understood as capabilities essential for participation in society and markets. Its governance should prioritize respect for fundamental rights and ensure inclusive benefits. However, the reality of DPI implementation in Africa today reveals a conflict between its envisioned purpose (maximizing inclusion and agency) and its practical application (state function and control).

The Technocentric Trap: A key challenge identified in this study is the dominance of technocratic thinking in the development of DPI. Policymakers frequently prioritise technological capabilities such as interoperability, automation, and biometric precision, while paying insufficient attention to the social, cultural, and economic contexts that shape digital access. This creates systems designed around an assumed universal user who is literate, digitally confident, securely connected, and politically unencumbered, despite the fact that many citizens operate under very different conditions. Women's digital access, for example, is mediated by patriarchal norms, unequal household power, limited financial independence, and lower levels of digital literacy. When DPI is built without acknowledging these realities, exclusion becomes embedded in the system's design.

Digital Authoritarianism and Evasion of Accountability: The expansion of DPI has also occurred alongside an increase in digital authoritarian practices across the region. Internet shutdowns, heightened online surveillance, data misuse, and opaque partnerships between governments and private companies have become worrying trends. In contexts lacking strong democratic safeguards, DPI can inadvertently extend state overreach and control into everyday life through mechanisms such as:

- **Surveillance and Suppression:** African countries have seen a rise in internet shutdowns (21 incidents in 15 countries in 2024 alone). Surveillance laws, such as Zimbabwe's 2025 Cyber and Data Protection Act, enable real-time monitoring of citizens.
- **Aggregated Power and Distrust:** Citizen trust in government data processes is low due to a lack of transparency and fears regarding data use. In Kenya, private sector collaboration has been alleged, with aggregated database information (including from mobile money services like M-Pesa) used to track and target citizens during protests. This lack of accountability leads citizens to view certain DPI initiatives with suspicion.

Digital Public Infrastructure's Failure to Account for Systemic Inequality

Systemic inequalities including low education levels, high economic vulnerability, and the digital gender divide, are often reinforced or worsened by DPI systems that fail to address these intersectional realities.

Entrenched Gender and Identity Discrimination: DPI systems perpetuate exclusion by reinforcing existing patriarchal and discriminatory legal structures:

- **Institutional Misogyny in ID:** In several African nations, patriarchal norms are legally reflected and reinforced, requiring women to obtain male authorization (from a husband or guardian) to secure critical documents like passports or to sign contracts. This institutional misogyny effectively treats women as lesser individuals and marginalizes them from foundational ID systems.
- **Exclusion of Minorities:** The process of obtaining a national ID is fundamentally political from the citizenship perspective. Ethnic minorities, including Somali and Nubian groups for example in Kenya tend to face brutal vetting processes and arbitrary citizenship denials based on colonial logics and political ends. This exclusion denies them their enjoyment of fundamental rights that come with citizenship.

Flawed Design and Increased Vulnerability: When DPI systems are confusing, inaccessible, or mistrusted, citizens, especially women, often turn to intermediaries for assistance with registration or transactions. This reliance exposes them to a higher risk of fraud, data theft, coercive fees, and exploitation. In many households, women lack full control over their own devices or accounts, meaning DPI may inadvertently deepen financial dependency or compromise personal safety.

- **The Problem of the 'Universal User':** South Africa's MyMzansi roadmap frames its "universal user" (Thandi) as educated, digitally literate, and connected. This framework fails to represent the majority of vulnerable citizens, especially unemployed Black women in rural areas who face high economic vulnerability and low rates of internet use. This approach risks MyMzansi being exclusionary by design.

- **Digital Payments and GBV Risk:** While digital payments (like M-Pesa in Kenya) have driven financial inclusion, they do not guarantee universal agency. In rural areas, women's access to devices and control over income flow are often monitored and controlled by male household members. Crucially as well, women's growing financial independence enabled by digital systems in South Africa has been linked to increased household conflict, resulting in Gender-Based Violence (GBV) and femicide. Policymaking rarely recognizes these issues as risks to mitigate within DPI deployment in the African context.

Policy Recommendations

Ultimately, this study advances the thinking that to realize the inclusive potential of DPI, policy must adopt a rights-first, structurally corrective approach across all levels of implementation and governance.

To policy makers and governments regulatory actors

- **Mandate Rights-Respecting Design:** Governments need to transcend beyond universal and gender-neutral mechanisms that reinforce marginalization. Adopt "gender by design" frameworks that capture intersectional differences (including income, education, and care labour) and use multiple user personas, eschewing the flawed one-size-fits-all universal user concept.
- **Dismantle Discriminatory Legal Barriers:** Prioritize legislative reforms to challenge and repeal discriminatory laws concerning nationality, birth certification, and passport requirements that necessitate male authorization. Legal frameworks must ensure the preservation of rights concerning data privacy, non-discrimination, and decisional autonomy.
- **Treat Access as an Economic Right:** Getting women properly engaged into digital financial services is a core economic right that drives wider socio-economic growth. That means going all-in on last-mile outreach, with substantial human intervention to actually reach rural women and girls who are usually left behind
- **Promote Trust and Accountability:** Citizens won't use Digital Public Infrastructure if they don't trust it. Regulators need to build public confidence by setting up clear, independent oversight bodies and easy-to-use complaint and redress systems for redress when citizens' rights are infringed upon through interaction with DPI systems.
- **Integrate Social Realities into Risk Mitigation:** It's not enough for regulators to focus only on the tech-side rules. They need protections that also address hidden dangers, such as entrenched patriarchal control or the increased GBV triggered by women's digital financial independence.
- **Support Evidence-Based Implementation:** Regulators and public institutions should actively back Civil Society Organizations in developing solid evidence through real-world user experience research and detailed, granular evaluation frameworks. It's precisely this body of evidence that will allow everyone to truly grasp both the qualitative and quantitative effects that Digital Public Infrastructure systems have on marginalized and underrepresented communities at every stage of the implementation process.

Conclusion

The governance of Digital Public Infrastructure is more than just a technical exercise but rather a critical reflection of a society's commitment to democratic values and structural equity. If power dynamics are left unchecked, DPI risks becoming a mechanism for reinforcing existing societal cracks, acting less like a ladder toward inclusion and more like a high-tech filter that locks underrepresented communities permanently outside the digital economy.