ecdpm

DISCUSSION PAPER No. 412

The political economy of digital public infrastructure in Africa

By Melody Musoni

November 2026

As the rollout of digital public infrastructure (DPI) surges globally, African countries are increasingly adopting DPI policies and strategies to accelerate digital transformation, regional integration and public service delivery. While continental frameworks and regional initiatives have long embedded DPI's foundational pillars of digital identity, digital payments, and data exchange, thus preceding the contemporary DPI push, this introduces complex political economy dynamics.

This paper examines these dynamics to discuss who truly benefits from the DPI surge as it is currently being pursued. Although governments leverage DPI for administrative efficiency and service delivery, weak safeguards and the absence of robust data protection risk enabling state surveillance and citizen exclusion. Multinational technology companies often capture a disproportionate share of the commercial value generated by DPI, notably via the underlying cloud infrastructure, reinforcing external dependencies and creating risks of vendor lock-in. Conversely, the collection and processing of citizens' personal and biometric data, coupled with inadequate data protection safeguards and weak cybersecurity measures, pose risks to citizens' privacy, increase the potential for biometric data misuse, and expose citizens to cyber threats.

To ensure DPI genuinely serves African societies, policymakers must move beyond standardised, externally driven models. Key recommendations include making public value the primary test for DPI deployments, rigorously enforcing personal data protection and cybersecurity safeguards, aligning DPI initiatives with national and regional development priorities under the AfCFTA, and anchoring projects in a coherent multi-stakeholder governance.

Table of contents

Acknowledgements **2**
Acronyms **3**
Executive summary **4**
Introduction **7**
The DPI promise **8**
Understanding DPI within the African context **9**
The political economy of DPI **13**
Who benefits from the DPI surge? 14
DPI: A win-win for governments 15
The distribution of DPI economic value 17
Without safeguards, citizens are the losers 20
Policy recommendations **22**
Make public value the primary test for DPI 23
Build DPI around national (or regional) priorities and not a standardised model. 23
Establish a coherent national digital vision 24
Protection of personal data should remain a top priority 24
Prioritise cybersecurity and prevent misuse 25
References **25**

Acknowledgements

I would like to thank Bruce Byiers and Chloe Teevan for their valuable insights and extensive feedback, all of which greatly strengthened the paper. The views are those of the author and do not represent the position of ECDPM. All errors remain those of the author. Comments and feedback can be sent to Melody Musoni (mmu@ecdpm.org).

Acronyms

ADC	Africa Digital Compact
AfCFTA	African Continental Free Trade Area
AI	Artificial Intelligence
AU	African Union
AWS	Amazon Web Services
DPI	Digital public infrastructure
DTS	Digital Transformation Strategy
EAC	East African Community
EARDIP	Eastern Africa Regional Digital Integration Project
G20	Group of Twenty
GDC	Global Digital Compact
ICT	Information and Communication Technology
ID	Identity
IMF	International Monetary Fund
NITDA	National Information Technology Development Agency
REC	Regional Economic Community
SADC	Southern African Development Community
SATA	Smart Africa Trust Alliance
SDGs	Sustainable Development Goals
SIM	Subscriber Identity Module
UN	United Nations
UNDP	United Nations Development Programme
US	United States
WARDIP	West Africa Regional Digital Integration Project
WURI	West Africa Unique Identification for Regional Integration and Inclusion

Executive summary

Digital public infrastructure (DPI) has emerged as a major global approach to digital transformation and is increasingly shaping how governments, development partners and technology companies engage with Africa's digital agenda. It is promoted as a means of improving public service delivery, interoperability, financial inclusion and digital economic integration. However, its growing prominence also raises important political economy questions about who defines priorities, who finances and builds the infrastructure, who captures the economic opportunities, and how data, technology and public interests are governed.

This paper argues that DPI is not entirely new to Africa. Long before the term gained global policy prominence, the African Union (AU) had already identified many of its core components through frameworks such as the Digital Transformation Strategy, the Data Policy Framework, the Interoperability Framework for Digital ID and the African Continental Free Trade Area (AfCFTA) Protocol on Digital Trade. Digital identity, interoperable systems, cross-border payments, data flows, privacy and open standards were already part of Africa's digital transformation agenda. What is relatively new is their consolidation into a distinct "DPI approach" and the growing influence of international actors promoting and financing this model.

The adoption of DPI across Africa is therefore not taking place in a political vacuum. African governments have clear incentives to develop interoperable digital systems, including improving service delivery, reducing administrative costs, strengthening tax administration, combating fraud, expanding social protection and generating better data for policymaking and innovation. DPI may also create opportunities for domestic technology firms and help countries build stronger data ecosystems that can support artificial intelligence and other forms of digital innovation.

At the same time, the direction of DPI is shaped by a wider group of actors, including development finance institutions, international organisations, bilateral partners, philanthropies and global technology companies. These actors can influence which projects receive financing, what technological models and standards are adopted, and which firms participate in implementation. While such partnerships can provide valuable financing and expertise, they may also reinforce structural dependencies. Domestic firms are often better positioned in applications and user-facing services, while more strategic and capital-intensive layers such as cloud infrastructure, systems integration and specialised cybersecurity remain concentrated among large global technology companies.

Open standards, interoperability and open-source technologies can reduce some forms of lock-in, but do not eliminate these broader market asymmetries.
The consequences for citizens require particular attention. The same systems that can improve access to public services can also increase the capacity of governments to collect, combine and analyse personal data. Digital ID and interoperable databases may create risks of surveillance, function creep, data misuse and exclusion, particularly where biometric systems are introduced without adequate legal safeguards and oversight. People without foundational identity documents, residents of border communities and individuals whose biometrics cannot be reliably captured may also be excluded from services when digital ID becomes a gateway to access. Data protection and other safeguards are therefore not supplementary concerns; they are essential to whether DPI delivers public value.

The paper makes five central recommendations:

1. **Anchor DPI in African priorities**: African governments should define how DPI supports their own national and regional development objectives. External financing should support domestically determined priorities rather than steer countries towards donor preferences, foreign technologies or standardised models.
2. **Make public value the primary test**: DPI investments should be judged by the tangible value they create for citizens. Governments should prioritise use cases that respond to concrete social and economic needs, ensuring that objectives such as improving tax administration, strengthening public sector oversight and enhancing state administrative capabilities are pursued alongside tangible benefits for citizens, rather than becoming ends in themselves.
3. **Build DPI around country context, not a universal model:** Priorities should reflect each country's development needs, institutional capacity, digital maturity and existing infrastructure. For some countries, the immediate priority may be foundational identity. For others, connectivity, digitisation of records or strengthening existing government systems may be more urgent.
4. **Establish a coherent national digital vision:** DPI should be integrated into broader digital transformation strategies and connected to data governance, cybersecurity, sectoral platforms, digital government programmes and existing regulatory frameworks. Clear governance structures should define institutional mandates, accountability and decision-making.
5. **Treat data protection and cybersecurity as foundational:** Personal data processing should have a clear legal basis and defined purpose. DPI

projects should incorporate data protection impact assessments, privacy by design, cybersecurity safeguards and effective oversight from the outset.

Ultimately, the key question is not whether African countries should adopt DPI, but on whose terms and towards what objectives. DPI can support more effective public services, stronger digital economies and greater regional integration, but these outcomes will depend on whether African governments retain agency over their digital priorities, strengthen domestic capabilities and ensure that citizens remain the principal beneficiaries of digital transformation.

Introduction

Digital public infrastructure (DPI) has gained prominence in global digital transformation policies, with governments, development partners and international institutions increasingly adopting it as a key approach to advancing digital development. These actors promote DPI as a means of expanding access to public and private services, strengthening interoperability between digital systems, fostering innovation and financial inclusion, and supporting the integration of digital economies. For African governments, the growing international emphasis on DPI presents both opportunities and raises important policy questions. African countries have already established digital transformation priorities through continental, regional and national strategies, including the AU Digital Transformation Strategy and Agenda 2063. The increasing prominence of DPI therefore raises questions about who shapes this emerging policy agenda, whose interests it serves, how it aligns with Africa's existing digital transformation priorities, and whether it offers additional value beyond ongoing digitalisation initiatives.

The DPI approach gained traction during the Covid-19 pandemic. India, which had already developed extensive digital systems for identification, payments and delivery of social protection through its Aadhaar digital ID and Unified Payments System, used this success story as a value proposition to position itself as a global leader on DPI. India elevated the DPI concept globally during its G20 presidency in 2023, carried on by Brazil and South Africa during their subsequent presidencies in 2024 and 2025. Importantly, DPI was presented not only as an Indian success story, but also as a developmental model emerging from the Global South that could offer relevant and adaptable solutions for other developing countries. This framing strengthened DPI's appeal as an example of innovation from the Global South for the Global South.

DPI became a global agenda when world leaders met at the Summit of the Future in 2024 (UN, N.d.b) and endorsed the Global Digital Compact (GDC)(UN, N.d.a). The GDC highlighted the role of resilient, safe, inclusive, and interoperable DPI as a means to deliver services at scale and increase social and economic opportunities for all. Following the GDC, governments committed to promote public sharing of DPI best practices and use cases, increase investment in digital public goods and DPI, especially in developing countries, and foster multi-stakeholder partnerships to design and scale DPI solutions.

DPI is also increasingly becoming the language through which global organisations like the World Bank, UNDP, multilateral institutions, and technical partners are engaging African governments on their digital agendas. Donors, philanthropic organisations and international nonprofits such as the Gates

Foundation, Co-develop, Mastercard, Omidyar Network, the Digital Public Goods Alliance and the Digital Impact Alliance are also prioritising DPI as a tool for inclusive digital development. Use cases in areas like agriculture and health are being promoted as a way of demonstrating the value offered by DPI (Burke, 2026; Roberts, 2025; WB, 2025; Totolo, 2025).

The growing role of several international organisations and technology partners raises questions about who defines DPI priorities, who finances and builds the underlying systems, who captures the resulting economic opportunities, and how decisions over data and infrastructure are governed.

This paper examines how African countries are engaging with the DPI approach, and how DPI, as both a concept and a policy framework, is shaping the types of digital systems being developed, the ways in which they are governed, and Africa's position on digital and data sovereignty. It also discusses the extent to which DPI supports Africa's regional digital integration efforts. That requires a deeper understanding of how the African Union, AU member states, regional institutions, international development partners, multilateral organisations and technology companies interact around the DPI agenda, the interests that drive their engagement, and their influence on Africa's institutional priorities, data governance, and market opportunities. While DPI promises to leapfrog traditional infrastructure deficits and support regional economic integration, its current trajectory also raises concerns about social exclusion, data exploitation and weakening Africa's digital sovereignty by deepening its dependency on a limited number of foreign technology providers.

The DPI promise

The DPI agenda is commonly framed as interoperable digital systems, using open standards and specifications to make the exchange of data between systems seamless. DPI can be open source, but is not necessarily so. The three pillars most commonly associated with DPI are: digital identity; digital payments; and data exchange. Together, these provide the basis for providing public societal functions, offering digital rails through which data can be securely exchanged. A good illustration of DPI in practice is that citizens can use their unique digital IDs to access government e-services and, through that same platform, pay their taxes or receive payments of benefits and salaries. Although these three DPI pillars have become the dominant global framing of DPI, they should not be treated as a fixed model, but each country should build DPI based on its own priorities, contexts, and institutional needs (Teevan et al., 2025).

While many of DPI's core components predate the use of the term, the concept has increasingly been used to describe these foundational systems as shared infrastructure on which multiple public and private services and applications can be built. Its growing relevance is linked to the need to address persistent challenges including financial exclusion, inefficient public administration, limited access to social services, revenue leakage, fraud and weak identity verification. Digital ID and payment systems can reduce the cost of customer identification and transactions, widening access to financial services, while interoperable government systems can improve tax collection and other forms of public revenue mobilisation.

DPI can also enable governments to identify eligible beneficiaries and deliver social protection and other services more rapidly. During COVID-19, countries with interoperable digital systems were able to reach up to three times more people with emergency cash assistance. Togo's Novissi programme used digital systems to provide direct transfers to citizens who had lost income (Musoni et al., 2026). Greater integration of government data can also strengthen transparency and reduce fraud. Biometric verification contributed to the removal of approximately 62,000 ghost workers from Nigeria's public payroll and 10,000 in Zimbabwe (Musoni et al., 2023). Reliable identification can additionally support safer access to services by enabling individuals to prove who they are, although such systems must include safeguards against exclusion, surveillance and misuse.

More broadly, DPI can lower administrative costs. Estonia's e-government infrastructure is a good example, where it is estimated to save around 2% of GDP annually through reduced paperwork (Eaves and Vasconcellos, 2025). DPI can also facilitate trade, mobility and regional integration, as illustrated by the EU's eIDAS framework for mutual recognition of electronic identities hopes to do (EC, 2025). These benefits, however, depend on DPI being designed not merely as an efficiency or cost-saving tool, but as inclusive public infrastructure that embeds transparency, accountability, participation, privacy and citizen empowerment from the outset (Eaves and Vasconcellos, 2025; Mazzucato et al., 2024).

Understanding DPI within the African context

A review of digital policies of the AU shows that Africa was building DPI pillars before the term 'DPI' gained global policy prominence, even if their approach to building these digital rails was different. Through strategies like the Digital Transformation Strategy 2020 -2030 (DTS)(AU, 2020), the African Union (AU) already identified the foundational pillars needed to build the African digital economy. These foundational pillars include digital infrastructure, digital innovation and entrepreneurship, digital skills and human capacity, and an

enabling policy and regulatory environment. Digital identity (digital ID) for citizens, cross-border digital payments and data flows, open standards and interoperability, and protection of personal data and privacy are identified as critical enablers needed to build the African digital economy. The AU further developed the Interoperability Framework for Digital ID[1] (which focuses on mutually recognised digital ID)(AU, 2023), and the AU Data Policy Framework[2] (which promotes cross-border data flows)(AU, 2022) and the AfCFTA Digital Trade Protocol[3] (with several annexes supporting digital ID, data exchange, cross-border payments, among others)(AU, 2024a). Throughout the development of these continental policies and frameworks, DPI was not yet explicitly recognised and integrated as 'an approach' to how African countries implement digital transformation. Nevertheless, its core pillars are clearly embedded within them.

The Africa Union's priorities have never centred on the three DPI pillars but were much broader, focusing on creating the enabling policy and regulatory environments, supporting digital infrastructure for connectivity and cloud, empowering citizens with digital skills, and creating opportunities for innovation and entrepreneurship. This broader framing is important. A narrower focus only on the DPI pillars risks distracting from the real objective: to promote inclusive, safe and secure digital development. It may also marginalise or overlook earlier or ongoing digitalisation efforts simply because they are not explicitly labelled as DPI or fall under one of the three pillars (Sridharan et al. 2024).

The first instrument where the AU explicitly mentioned DPI is the AU Africa Digital Compact (ADC)(AU, 2024b). The ADC was developed as Africa's contribution to the text shaping the Global Digital Compact. Mirroring the GDC's language, the ADC states that DPI can help '*...maximise the opportunities for digitalisation to support the UN SDGs and the AU Agenda 2063 while reducing the risks that digital technologies may spark off.*' However, the ADC does not clearly define what DPI means within the African Union context, suggesting that the concept was adopted more as an externally-driven broad framing than as a fully owned and elaborated AU policy concept.

DPI and regional coordination: From policy to practice

As momentum has grown around the DPI agenda, African regional institutions and regional economic communities (RECs) have increasingly begun to

[1] The AU Interoperability Framework for Digital ID adds a continental framework for mutual recognition and interoperable digital credentials where Africans can easily and securely access services and participate in the digital economy and society with greater trust and certainty.
[2] The AU Data Policy Framework focuses on data governance, including cross-border data flows.
[3] The AfCFTA Digital Trade Protocol which creates the African digital single market, does not include references to DPI as an approach to build the DSM. Instead, the protocol has detailed annexes covering cross-border data transfers, digital identities and cross-border digital payments.

incorporate DPI-related priorities into regional digital integration strategies and implementation frameworks. The Southern African Development Community (SADC) developed the SADC Digital Transformation Strategy aligned with the AU DTS. The East African Community (EAC) developed a Data Governance Policy, Cross-Border Payments Masterplan, and moved further in explicitly framing DPI as a regional integration instrument. Its 2025 Digital Public Infrastructure Needs Assessment (the drafting of which ECDPM supported) explicitly frames DPI as a means to support regional economic integration, improve service delivery, and unlock shared infrastructure and use cases across partner states. The report identifies practical regional opportunities, including cross-border payments, digital trade facilitation, mutual recognition of qualifications, health-data use cases, and identity portability.

Beyond the RECs, the Smart Africa Alliance has developed a series of practical blueprints that translate broad digital transformation ambitions into more operational guidance. These include the Digital Identity Blueprint focused on interoperability and mutual recognition, the Digital Economy Blueprint that integrates DPI, and the e-Payments Blueprint focused on cross-border payments, standards, and enabling infrastructure. During the Transform Africa Summit of 2025, Smart Africa Trust Alliance (SATA)(2025) was identified as a key enabler to support African governments to build connected operating systems that enable interoperability, secure data exchange, and seamless service delivery across borders.

The continental and regional policies are complemented by a number of projects and initiatives aimed at operationalising elements of DPI in practice. For instance, the World Bank supported the Eastern Africa Regional Digital Integration Project (EARDIP)(EAC, 2025) and West Africa Regional Digital Integration Project (WARDIP)(Sanchez Vigueras, 2021). Both aim to advance digital market integration in the respective regions by increasing affordable access to regional broadband connectivity and strengthening the enabling environment for cross-border digital services. The West Africa Unique Identification for Regional Integration and Inclusion (WURI) program is another project driving interoperable, inclusive ID systems to enable cross-border access to services and jobs (ECOWAS, 2022).

Taken together, these initiatives suggest a gradual shift from high-level digital transformation strategies towards more concrete regional frameworks for implementing DPI as a means to regional integration.

DPI at the national level

At the national level, fewer African countries have adopted explicit DPI approaches. South Africa developed a DPI roadmap which sets out a phased,

whole-of-government approach centered on digital identity, data exchange, and digital payments (South Africa DPI Roadmap, 2025). The roadmap defines DPI as multi-purpose technology building blocks that provide the foundation for various government services and describes DPI as the 'spine' of South Africa's digital transformation of government. During the Global DPI Summit, South Africa's Minister for Communications and Digital Technologies launched the MyMzansi platform, the country's DPI platform for citizens to access government services.

Rwanda has positioned itself as a continental leader by establishing a Centre for Digital Public Infrastructure to support governments, civil society, and the private sector in deploying secure and scalable digital systems (RISA, 2025). The center will also serve as a dynamic testbed for emerging DPI solutions, allowing innovators to pilot and refine technologies before large-scale implementation. Rwanda's ICT Sector Strategic Plan (2024–2029) aims to improve operational efficiency by developing and implementing frameworks for DPI development, deployment, and operation, and DPIs that improve the quality of service delivery (RISA, 2025).

Kenya has also embarked on developing its DPI Roadmap, with the support of ECDPM and GIZ. The Roadmap sets out a ten-year strategy for transforming public service delivery through integrated digital systems, secure data exchange and inclusive digital identity. The Roadmap aims to position Kenya as a leader in digital government in Africa while improving the efficiency, transparency and accessibility of public services for citizens, businesses and public institutions. The roadmap builds on a broader policy and institutional framework that includes Kenya's National ICT Policy, the Digital Economy Blueprint and the Kenya National Digital Master Plan, all of which promote connectivity, digital inclusion, interoperable government systems, shared platforms, digital skills, innovation and a coordinated whole-of-government approach to digital transformation. To strengthen DPI, the Government of Kenya also adopted the Government Digital Enterprise Architecture, which establishes common standards and reference models for public sector business processes; the Interoperability Framework, which guides systems integration and data exchange across government institutions; and the Data Governance Policy, which seeks to promote consistent standards for data stewardship, secure data sharing, institutional accountability and trusted use.

Recently, Nigeria's National Information Technology Development Agency (NITDA) developed draft Technical Standards for DPI (Akintaro, 2025), which laid the foundation for a whole-of-government approach to reforming public service delivery and engaging stakeholders to develop a DPI roadmap (Alao, 2025). All these activities might also culminate in the development of a Nigeria Stack and National Policy on DPI, which was proposed by the Federal Ministry of

Communications, Innovation & Digital Economy to create synergy across the three DPI pillars and close the digital gap between citizens, businesses and government (FMCIDE, 2023).

The discussion above shows that the core pillars of DPI have long been embedded in the African Union's broader digital transformation frameworks, even if they were not articulated holistically as a distinct 'DPI approach'. African countries and regional bodies are now increasingly adopting DPI explicitly as an approach to digital transformation. Given this upsurge in DPI strategies across Africa, the following section explains *why* this shift towards the 'DPI approach' is taking place, who is behind it, whose interests it reflects, and how its benefits and risks are distributed.

The political economy of DPI

The adoption of DPI is not taking place in a political vacuum but is shaped by domestic and international interests, priorities and incentives (Totolo, 2025). While DPI has gained significant international momentum, particularly following the 2024 Global Digital Compact, questions remain about what really drives the agenda and the extent to which the global DPI agenda aligns with African countries' national digital transformation priorities. The interests and priorities of African countries concerning the different pillars of DPI are not always articulated, creating opportunities for influential domestic and external actors including technology providers, donors and development agencies to shape national DPI agendas. Acknowledging these dynamics is important for understanding who influences DPI adoption, investment and implementation decisions, and how national priorities are negotiated within the broader global DPI agenda. This section raises the key political economy considerations shaping the adoption and implementation of DPI in Africa.

As a whole-of-government and whole-of-society approach, DPI development depends on political buy-in and prioritisation at the highest levels of government. But its implementation then reflects the interaction of a range of strategic and key government ministries and agencies with different interests and incentives, including finance, health, social welfare and ICT ministries, central banks, ID agencies, tax and revenue authorities, and data protection agencies. As well as their role in demonstrating the public value of DPI, its rollout can create 'winners' and 'losers' whether in financial terms or in terms of political power . Beyond government institutions, global technology companies, philanthropies, development agencies and political and economic elites have a vested interest in the digital ecosystem and have influence over which DPI projects get prioritised,

the governance models adopted and the applicable technical standards and indeed solutions adopted.

Citizens are directly affected by these decisions about how DPI systems are designed, governed and rolled out, especially where these systems involve large-scale collection and linking of personal or biometric data or become gateways to essential public services. Weak safeguards, limited transparency, and concerns over privacy and security can undermine public trust and lead citizens to perceive DPI as a tool of surveillance rather than as infrastructure that improves access to services and administrative efficiency (Totolo, 2025). Kenya's attempted rollout of the Huduma Namba digital ID system is a good example. It shows the clash between the government's ambition to massively collect biometric data and develop a digital ID and the resistance from the citizenry who have no trust in the digital ID system. The initiative sought to establish a centralised identity system drawing on extensive personal and biometric data, but faced sustained legal and civil society challenges over privacy, data protection and exclusion. In 2021, the High Court of Kenya quashed the government's decision to roll out Huduma Namba and found that the rollout had proceeded without a data protection impact assessment required under Kenya's Data Protection Act and ordered the government to undertake such an assessment before proceeding (Privacy International, 2022).

Better understanding the political economy of DPI in Africa may help to show what countries really need in order to develop their digital ecosystems, how to go about implementing DPI projects, who to partner with, whose buy-in is needed and how to secure it, how to develop digital governance frameworks and how to ensure sustainability.

Who benefits from the DPI surge?

DPI is an approach to promote inclusive social and economic development for societal benefits through access to services. Countries like South Africa are using DPI as a tool to facilitate social protection services and to help citizens to get access to government services fast and efficiently. Whether a country is upgrading its existing digital infrastructure (brownfield) or building new digital infrastructure systems (greenfield), DPI is viewed as offering a way to promote interoperability, reduce duplication, improve service delivery, and potentially lower costs in the long run. India, which built its DPI systems from scratch, has highlighted DPI as a way to promote financial inclusion and promote economic development, including through home-grown ecosystem development. Brazil, in contrast, has adopted DPI thinking as a means to build interoperability between

existing homegrown systems that were not initially considered DPI (Teevan et al., 2025).

Just as India and Brazil each steered their own paths, the different political, economic and social dynamics across Africa mean that it too should steer its path, and that DPI development in Africa cannot take the same pattern or trajectory as in other regions.

In political economy terms, DPI strategies and policies represent a set of 'formal institutions' with a strong technical logic, while their rollout is then subject to 'informal institutions'—the informal 'rules of the game' that govern political and economic relations within or between states. Different actors, or stakeholder groups, then operate within this combination of formal and informal rules, where political, administrative, private and citizen interests and power may not align with the stated goal of widening citizen benefits.

DPI's current trajectory is shaped by a variety of different global actors. Roberts argues that although DPI is presented in terms of its benefits to citizens, its expansion also serves the political, commercial, institutional, and geopolitical interests of governments, technology companies, international organisations like the IMF and World Bank, and philanthropies (2025). These powerholders possess the financial resources, institutional authority, and policy networks needed to shape how DPI is understood, funded, and implemented across Africa. Through direct funding to governments,providing technical assistance, supporting civil society groups and research institutions, convening policy dialogues, and financing research and pilot projects, these powerholders can shape which problems are framed as priorities, which technological approaches receive support, and which models of DPI gain legitimacy. This helps explain the rapid diffusion of DPI across development policy, international conferences, civil society programmes and academic and policy research. This does not mean that these actors share the same interests or agendas or that their influence is negative, but while DPI is primarily justified in terms of improved public services, inclusion and development, its expansion can also generate benefits for the actors that finance, design, supply and promote these systems. This makes the question of agenda-setting important and relevant.

DPI: A win-win for governments

On paper, governments developing DPI use cases are interested in finding ways that DPI can make their systems more transparent, accountable, efficient, and cost-effective. Areas that governments prioritise include taxation, social security protection, combatting corruption, fraud and mismanagement of public funds. In

countries like Nigeria and Zimbabwe, the use of digital ID helped to get rid of ghost workers, addressing and promoting transparency (Musoni et al., 2023). In South Africa, which faces a surge in the number of undocumented foreigners, the introduction of digital ID is seen as an effective way to curb identity theft and ensure that the right people receive government social protection (Republic of South Africa, 2024; Republic of South Africa, 2026).

The collection of biometric data for digital ID and the interoperability of systems comes with the risk that governments can more easily surveil citizens and entrench state power (Sani, 2025; CIPESA, 2024; Sesan and Roberts, 2025). Governments can use the combined data from ongoing smart city initiatives, blended together with interoperable DPI systems, for surveillance, policing and intelligence. The fear for many is that this panoptic surveillance gives governments power to control their citizens, politically manipulate them, and even decide who gets social assistance and who does not (Mare and Roberts, 2024; Carp, 2025). These developments raise concerns about what Scott describes as state legibility, referring to the ability of states to make populations more visible, identifiable and administratively manageable (Scott, 1998). The risks with DPI are that efforts to make citizens more legible to the state may prioritise administrative efficiency and state control at the expense of privacy, data protection and individual autonomy, particularly where adequate governance and accountability safeguards are absent.

Although DPI systems involve the processing of large amounts of personal data, most projects neglect to include safeguards and guardrails to protect personal data. Many development partners and donors funding DPI projects do not make personal data protection compliance a prerequisite for financing, with few exceptions[4]. As a result, digital ID programs and wider DPI projects are being implemented first, with protection of personal data as an afterthought. Instead of insisting on privacy by design and default, or human rights and data privacy impact assessments, DPI programs often prioritise other benefits. This approach to funding DPI adoption does not encourage African governments to prioritise data protection, though many African countries still do not have sufficient data protection laws or enforcement capabilities.

DPI also presents an opportunity for Africa to transition from 'data deserts' to 'data streams.' Data has many potential usages for public good, but the growing availability and economic value of data also raise important questions about privacy, equitable access, commercialisation and the distribution of benefits. For

[4] The European Investment Bank made enactment and effective implementation of a data protection law a condition for it to co-finance Nigeria's Digital Identification for Development project.

a long time, the data landscape in Africa has been described as 'data deserts' due to the absence of digitised government records, lack of up-to-date datasets, and unreliable data sources (Ndemo et al., 2023). The introduction of interconnected digital systems presents an opportunity for African governments to collect and collate data in real time and build new datasets. Data is the 'digital soil' for innovation, and DPI is likely to help African countries build stronger and more valuable domestic data ecosystems. Most governments now have a better understanding of the value of African data for innovation and AI and are exploring ways to utilise their data for economic benefit while also using it as leverage when negotiating with foreign firms and governments. For example, Kenya's Data Governance Policy proposes the establishment of a legally regulated national data marketplace for the lawful exchange of non-personal, anonymised and aggregated datasets across private and public sectors, research institutions and the private sector. While this proposed data value creation seems promising, there is a risk of re-identification of anonymised data, the commercialisation of data collected for public purposes, unequal access favouring large firms, and concentration of economic value among powerful intermediaries rather than citizens and communities.

These aspirations for data value creation also align with the AU Data Policy Framework and the AfCFTA, which seeks to create an enabling environment for innovation, entrepreneurship and data-driven economies while promoting interoperability and cross-border data flows in Africa. DPI can help translate these policy ambitions into practice by providing the shared technical, governance and trust mechanisms needed for secure and interoperable data exchange across borders. During South Africa's G20 Presidency, there was a call for DPI innovations from Africa which were aimed at showcasing how DPI advances regional integration, supports the AfCFTA and enables cross-border digital services and data exchange in Africa. As DPI expands and generates volumes of valuable data, firms controlling data may be well positioned to capture significant economic and strategic benefits because they control the infrastructure, the computing capacity, and the platforms used to collect, process, and commercialise data.

The distribution of DPI economic value

Private sector participation is integral to the development and operation of digital infrastructure, including DPI. Firms provide connectivity, cloud, software, systems integration, cybersecurity, identity technologies, payment services, etc. The private sector relevant to DPI is quite broad and includes big tech, telecommunications firms, domestic software developers, and fintechs, but these players all possess different financial, technological, and bargaining power. Understanding the political economy of DPI also involves understanding which

companies benefit and under what conditions. This is quite significant as many African governments continue to depend on foreign technology providers for significant parts of their digital infrastructure.

Opportunities for domestic firms and local innovators

DPI development in Africa is increasingly linked to broader ambitions to strengthen domestic technology ecosystems and support locally developed solutions (DPI, 2024). Kenya's M-Pesa is frequently cited as an example of how private-sector innovation transformed the payments ecosystem and expanded financial inclusion in Kenya. African governments are using public-private partnerships (PPPs) and other arrangements through which private firms help design, provide, test, or manage digital services and infrastructure. Kenya and Tanzania have used central bank-led regulatory sandboxes to test digital financial innovations, while Rwanda has developed a DPI sandbox through the DPI Center and has begun offering other countries access to this environment for experimentation and learning (Musoni et al., 2026). Team Europe has also set up a DPI Acceleration Mechanism under the EU-EAC Digital Economy, E-Commerce, E-Payment and Public eServices (DEEP) program to help DPI projects in EAC partner states become bankable and access financing. This opportunity is open to domestic companies pursuing DPI-related projects from data-sharing, digital ID, e-government, cybersecurity, etc. Such arrangements can support the testing of digital identity use cases, eKYC, payments and data exchange solutions before wider deployment. If designed with clear public-interest safeguards, PPPs can help mobilise investment, strengthen local innovation ecosystems and reduce the risk that DPI development becomes limited to large-scale procurement from established technology providers.

Big tech, market power and structural asymmetries

While there are some benefits generated by DPI for domestic firms, these benefits may be more limited in scale when compared to the value accrued by big tech and other foreign firms. Local firms may be well placed to develop applications, user-facing services and context-specific solutions. However, more capital-intensive and strategically important layers such as cloud infrastructure, large-scale systems integration, cybersecurity and other specialised technical services remain concentrated among a small number of global firms. For example, cloud infrastructure across the globe is highly concentrated among Amazon AWS, Microsoft, and Google, while companies like Huawei occupy important positions in telecommunications and digital infrastructure markets (Sridharan et al., 2024; Rikap, 2026). This raises an important question about who ultimately captures the most valuable opportunities generated by the various

interconnected digital systems supporting DPI. Many African governments rely on foreign technology providers for important components of their digital infrastructure, even as policy debates increasingly emphasise digital sovereignty and the development of domestic technological capacity.

Reliance on external providers is not problematic in itself. The concern arises where governments become structurally dependent on particular firms, making it difficult or costly to change suppliers. This is where questions of vendor lock-in and technological dependence become important. Open standards, interoperability and open source technologies are promoted as ways of reducing these risks because they can make systems easier to integrate, adapt and potentially transfer between providers. However, while they can reduce some forms of technical lock-in, they do not by themselves eliminate the wider market advantages enjoyed by large technology companies. What this means is that large technology firms may continue to enjoy significant advantages arising from scale, existing government relationships, technical capacity, access to capital and control over underlying infrastructure and services. These big tech firms have increased their participation in DPI and open-standards initiatives. For example, Google has positioned itself by offering its 'DPI in a box' program, which provides governments with packaged technical tools and support for building DPI components (Teevan et al., 2025). Open technical architecture may therefore make it easier for governments to avoid dependence on a single proprietary product, but it does not necessarily eliminate broader dependencies on particular firms to offer services such as hosting, maintenance, or specialist expertise.

Government-to-government partnerships and technology choices

More broadly, technology choices are not always made through conventional procurement processes alone. Countries like India and Estonia have actively promoted their digital government models internationally through government-to-government partnerships, development cooperation and other forms of digital diplomacy (Karanja, 2025; Hardy, 2020). However, these processes do not operate solely through bilateral arrangements. Development banks and other development partners also finance large digital transformation programmes and support the technical assistance, institutional reform and infrastructure development that precede formal procurement. For example, India is an influential actor in Africa's DPI development, and combines financial assistance with technical cooperation and knowledge transfer. It is currently supporting the African Development Bank (AfDB) to conduct DPI workshops across Africa and also promotes the Indian experience through high-level learning missions for senior African government representatives to engage with leading institutions such as UIDAI, NPCI, and NASSCOM. These intergovernmental

arrangements can shape the competitive process through which technologies and implementing partners would ordinarily be selected. The concern is that by the time procurement and contract negotiation teams become involved, important choices concerning architecture, technology providers, standards, financing models, and preferred implementation approaches may already have narrowed the range of available options.

Technical partners and development finance institutions may influence the design of digital systems, while government-to-government agreements may introduce preferred technological models or implementation partners. Procurement then takes place within a landscape that has already been partly shaped upstream. This does not mean that such arrangements necessarily undermine competition. Government-to-government cooperation and development-finance programmes can provide governments with access to expertise, technology and financing that would otherwise be difficult to obtain.

DPI governance must therefore extend both upstream and downstream. Upstream, governments need to assess how technology partnerships, development finance arrangements and technical assistance programmes shape architecture, standards and supplier choices. Downstream, procurement and contractual arrangements should preserve competition, interoperability and the ability to change suppliers. Requirements relating to transparency, data portability, technical documentation, interoperability, exit arrangements and skills transfer can reduce the risk that governments become dependent on individual providers over time (Clark et al., 2025; Chetty et al., 2025).

Without deliberate policies to support domestic firms, preserve competition and build public-sector technological capacity, DPI may expand digital markets while reinforcing existing concentrations of economic and technological power. With appropriate governance, procurement and capability-building measures, however, it can also create opportunities for domestic firms to participate more meaningfully in emerging digital ecosystems and strengthen local technological capacity.

Without safeguards, citizens are the losers

Although DPI is presented as a value proposition designed to improve public service delivery and benefit citizens, in practice it can generate significant risks and challenges that may outweigh its intended benefits. This concern is particularly acute in relation to digital identification systems, which can enable surveillance, data misuse, function creep, and the exclusion of individuals who lack documentation. The United Nations developed the DPI Safeguards

Framework, which offers practical, rights-based guidance for making DPI safer, more inclusive, accountable, and effective across its governance, design, deployment, and use (UNDP and ODET, 2026). However, in practice, DPI implementers tend to overlook these safeguards.

One of the concerns that citizens have with DPI is the gradual normalisation of digital ID as a prerequisite for access to online services. Digital ID may be justified where reliable identification is genuinely necessary. For example, when accessing social protection benefits, the government should know if the right beneficiary is accessing these benefits. However, there is a growing tendency for digital ID, particularly biometric digital ID, to become a universal gateway to participating online. Personal data protection principles such as data minimisation, proportionality, or necessity seem to be overlooked in some instances, as seen in the Kenya Huduma Namba example.

Many digital ID programs use fingerprints, facial images or other biometric characteristics during enrolment and authentication. The use of biometrics raises risks that are much more serious than the use of passwords and replaceable credentials. Biometric characteristics cannot be replaced after any data breach. Biometric data is now a pre-condition for obtaining a SIM card as well as for accessing mobile money or banking, which provides the state with the potential for real-time panoptic surveillance of every citizen's location, purchases, utterances, associations, and political preferences (Roberts, 2025). This is a major concern for citizens, especially those in countries where governments constantly threaten freedom of expression, speech, and political association.

Digital ID systems are centred around building these biometric databases, which can be accessed by several different entities to verify and confirm an individual's identity. The problem with this is that there is room for function creep and surveillance, and at the same time, if there are errors in biometric matching, then legitimate users can't access services. South Africa, for example, allows participating banks to verify customers against the Department of Home Affairs identification system using fingerprints, and there are now plans to allow telecommunication providers to get access to the digital ID system and verify customers when they register SIM cards (Fakiya, 2026).

The move to make digital ID verification compulsory during SIM card registrations is proposed as a response to cyber fraud, identity theft, and online scams. This approach to addressing cybersecurity concerns is not the most effective way to address the problem. Fraud arises from insecure databases, weak authentication processes, poor transaction monitoring, compromised devices, social engineering, inadequate consumer protection systems, or the failure of service

providers to respond to suspicious activity. While stronger identification may assist, it does not compensate for the deficient cybersecurity and may even create additional threats for individuals. Cybersecurity remains a significant but unevenly developed area across Africa, with many countries still facing gaps in legislation, institutional capacity, technical infrastructure, enforcement, and skilled personnel. Although some states have adopted cybersecurity strategies, data protection laws, and computer emergency response teams, studies show that implementation and preparedness remain inconsistent across the continent (Ifeanyi-Ajufo, 2023; Musoni, 2024; Snail ka Mtuze and Musoni, 2023). These weaknesses create particular risks for DPI platforms where large volumes of citizens' personal information, biometric and financial information are processed. The problem is compounded by limited public awareness and shortages of cybersecurity professionals, which reduce the ability of institutions and citizens to identify and respond to cyber threats.

Beyond privacy and security concerns, digital ID systems also tend to be exclusionary. Research shows that digital ID systems are exclusionary of people without foundational legal ID, border communities, and people who cannot be read by machines, like manual workers with 'faded' fingerprints (Mutung'u and Rutenberg, 2020; Mwanzia, 2021; Razzano, 2021). If these exclusionary challenges are not addressed, a DPI approach would mean that the same challenges are imported to new DPI platforms, thus leaving a significant number of the population without access to services.

The above discussion demonstrates that although digital ID offers significant social and economic benefits, it also exposes citizens to substantial risks. Personal data may be misused, subjected to further processing without lawful basis, commercially exploited, used for surveillance, or compromised through cyber threats and attacks. Where DPI is developed without adequate and enforceable data protection laws, privacy and security by design and default, effective cybersecurity safeguards, and inclusive governance mechanisms, the burdens and risks of DPI are disproportionately borne by individuals. In such circumstances, citizens may become the ultimate losers, as the benefits of DPI are undermined by weak accountability, inadequate protection and limited avenues for redress.

Policy recommendations

Digital public infrastructure is now a global policy agenda. It really matters for African countries to have a clear vision of how this global agenda aligns with their own national digital priorities. A lot of this requires clearly defining and articulating

their own interests and priorities, especially when engaging with donors and development agencies advancing the DPI agenda. African countries should make sure that external financing supports domestically determined objectives rather than steer policy towards donor preferences, foreign technologies, or externally designed solutions that may not reflect local needs and capacities. By doing so, African countries can take full control and give direction to how and which DPI projects are implemented within their country contexts.

The following policy interventions identify key measures for strengthening digital development in Africa while aligning DPI investments with national priorities, public value, institutional capacity, and long-term sustainability.

Make public value the primary test for DPI

African governments should prioritise making citizens the real beneficiaries of DPI. Instead of prioritising DPI use cases which can expand taxation or consolidate state control, governments should focus on how to create tangible value for citizens. This might require prioritising use cases that respond to real social and economic needs. For example, how DPI can help people without formal credit histories to access financial services, how cross-border travellers, displaced persons and refugees can easily carry their digital health records and access healthcare services, or how DPI can improve access to jobs and opportunities. Development agencies and funders should also conduct public-value assessments that identify intended beneficiaries, expected outcomes, possible harms and mechanisms for measuring whether benefits are equitably distributed before investing in DPI projects.

Build DPI around national (or regional) priorities and not a standardised model

African governments should resist the pressure to adopt a uniform model on DPI (centred on digital ID, payments and data exchange). Although it may be appealing for African governments to structure DPI around these three pillars, each country should determine its priorities according to its development needs, institutional capacity, digital maturity, existing infrastructure and socio-economic conditions. In some contexts, the immediate priority may be strengthening civil registration systems and ensuring universal access to birth certificates and identity documents. In others, it may be expanding affordable internet connectivity, digitising analogue records, or improving the reliability of existing government systems. DPI strategies should therefore be sequenced, context-specific, and grounded in nationally defined development objectives, while also aligning with regional priorities such as the AfCFTA.

Establish a coherent national digital vision

To demonstrate Africa's agency on DPI, governments should integrate DPI into a broader national digital transformation agenda rather than treat it as a separate policy framework controlled by a single ministry, agency or political office. Governments should clarify how DPI connects with existing data strategies, digital government programmes, sectoral platforms, data protection laws, cybersecurity policies and any relevant initiatives. At the same time, formal governance structures need to be put in place that can define institutional mandates, decision-making, accountability and give clear direction on DPI-related matters. This vision should be communicated consistently from top government to ministries, regulators, agencies and municipalities. Such communication helps low-level officials responsible for the actual implementation to understand DPI as an extension of existing digital investments, with greater emphasis on interoperability, reusable components and open standards. High-level political support should be matched by broad institutional ownership and meaningful participation by technical officials, local authorities, civil society, and communities throughout design, procurement, implementation, and oversight. Governments should also adopt change-management strategies, train public officials and procurement officers, and revise procurement rules that impede interoperability, vendor portability, and reuse of digital components.

Protection of personal data should remain a top priority

African countries still struggle with ensuring that data controllers and processors comply with their national data protection laws. Governments should ensure that DPI systems comply with requirements relating to lawful processing, purpose limitation, data minimisation, accuracy, transparency, storage limitation, security, and accountability. Any exchange or further processing of personal data across government departments or with private institutions should have a clear legal basis and be limited to specified purposes. DPI projects should undergo data protection impact assessments before deployment and whenever their scope or use changes. Privacy by design and by default should be embedded in system architecture, procurement requirements, contracts, operational procedures, and oversight arrangements. Consent-management tools may be useful in some contexts, particularly where individuals can make a genuine and informed choice about whether their data is shared. However, consent should not be treated as the sole basis for government data processing, especially where individuals depend on essential public services or lack a realistic ability to refuse. Citizens should be able to understand how their data is used, access and correct their records, challenge unlawful processing, and obtain effective remedies where harm occurs.

Prioritise cybersecurity and prevent misuse

African countries should also prioritise cybersecurity and public accountability. Governments should embed security by design and default, strengthen cybersecurity laws, incident-response capacity, independent audits, and public-private security obligations, while also ensuring transparent governance, independent oversight, and safeguards against surveillance, discrimination, exclusion and function creep. DPI systems should be subject to accessible complaint and redress mechanisms for individuals harmed by data breaches, unlawful processing, or inaccurate automated decisions.

References

African Development Bank. (2026). Call for DPI Consultant. AfDB.

African Union. (2020). Digital Transformation Strategy for Africa (2020–2030). Addis Ababa: AU.

African Union. (2022). AU Data Policy Framework. Addis Ababa: AU.

African Union. (2023). AU Interoperability Framework for Digital ID. Addis Ababa: AU.

African Union. (2024a). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. Addis Ababa: AU.

African Union. (2024b). African Digital Compact. Addis Ababa: AU.

Akintaro, S. (2025). NITDA releases draft Standards for Digital Public Infrastructure in Nigeria, seeks public input. Nairametrics.

Alao, O. (2025). NITDA Rallies Stakeholders in Co-Creating DPI, NGDX, for Effective Nationwide Digital Inclusion. National Information Technology Development Agency (NITDA).

Burke, M. (2026). The Political Economy of Digital Public Infrastructure Adoption in Digital Identity Systems. Polity, 8 May 2026.

Carp, T.-N. (2025). Mandatory Digital Identification and the Integrity of Democracy: Surveillance, Exclusion and the Risk of Authoritarian Revival. ResearchGate.

Chetty, P., Linder, T., Malik, P. and Rao, K. (2025). Towards an Integrated Data Governance Framework for DPI. T20 South Africa.

Clark, J., Marin, G., Ardic Alper, O. P. and Galicia Rabadan, G. A. (2025). Digital Public Infrastructure and Development: A World Bank Group Approach. World Bank.

CIPESA (2024). Biometrics and Digital Identity in Africa: Challenges, Opportunities and Policy Options. CIPESA.

D4D Hub. (2026). EAC DPI Acceleration Mechanism. D4D Hub.

DPI Africa. (2024). Why Safe and Secure Digital Public Infrastructure is Crucial for Africa's Future.

East African Community. (2025). EARDIP Objective and Strategic Components. Arusha: EAC.

East African Community (n.d.). Digital Transformation. (Accessed: 4 November 2026)

Eaves, D. and Vasconcellos, B. (2025). Digital Public Infrastructure is the New Global Tech Bet—But Everyone's Betting on Something Different. Tech Policy Press.

Economic Community of West African States (2022). West Africa Unique Identification for Regional Integration and Inclusion (WURI). ECOWAS.

Estonian Centre for International Development. (2024). Estonia is a valued development cooperation partner in Africa. ESTDEV.

Fakiya, V. (2026). South Africa wants every SIM to become a digital ID. Techpoint Africa, 21 July 2026.

Federal Ministry of Communications, Innovation and Digital Economy (2023). Accelerating Our Collective Prosperity through Technical Efficiency: A Strategic Blueprint for the Federal Ministry of Communications, Innovation & Digital Economy. FMCIDE.

Hardy, A. (2020). Estonia's Soft Power Through Technology. Atlas Institute for International Affairs.

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: At the crossroads of politics, sovereignty and cooperation. In: Policy Design and Practice, 6(2), pp.146–159. https://doi.org/10.1080/25741292.2023.2199960.

Karanja, R. (2025). The New Scramble for Africa: Digital empires, tech sovereignty, and the role of India, Estonia, GovStack, Brazil and other digital powers. Co-Develop.

Kenya ICT Action Network (2025). Kenya Launches Strategic Roadmap to Build Inclusive Digital Public Infrastructure (KICTANet).

MOSIP. (N.d.). Country Partners. MOSIP.

Musoni, M., Domingo, E. and Ogah, E. (2023). Digital ID systems in Africa: Challenges, risks and opportunities. Maastricht: ECDPM, Discussion Paper 360.

Musoni, M., Pouye, R. and Odhiambo, S. (2026). Digital Public Infrastructure in the East African Community. Maastricht: ECDPM, Discussion Paper 404.

Mutung'u, G. and Rutenberg, I. (2020). Digital ID and Risk of Statelessness. The Statelessness & Citizenship Review, 2(2), pp. 348 - 354. https://doi.org/10.35715/SCR2002.1111.

Mazzucato, M., Eaves, D. and Vasconcellos, B. (2024). Digital Public Infrastructure and Public Value: What is 'public' about DPI? Working Paper (WP 2024-05). UCL Institute for Innovation and Public Purpose (IIPP).

Mwanzia, S. W. (2021). Deploying Digital Identity Systems: Human Rights Implications and Lived Experiences in Kenya. Paradigm Initiative.

Ndemo, B., Ndung'u, N., Odhiambo, S. and Shimeles, A. (eds.) (2023). Data Governance and Policy in Africa. Palgrave Macmillan.

Razzano, G. (2021). AI4D – Digital and Biometric Identity Systems. Research ICT Africa.

Republic of Rwanda (2025). ICT Sector Strategic Plan (2024–2029). Ministry of ICT and Innovation (MINICT).

Republic of South Africa. (2026). Amendment of Identification Regulations, 1998. Department of Home Affairs, Government of South Africa.

Republic of South Africa. (2025). South Africa's Roadmap for the Digital Transformation of Government. Government of South Africa.

Republic of South Africa. (2025). DPI Innovation Accelerator Global Call for Submissions. G20 South Africa.

Republic of South Africa. (2024). White Paper on Citizenship, Immigration and Refugee Protection: Towards a Complete Overhaul of the Migration System in South Africa. Department of Home Affairs, Government of South Africa.

Roberts, T. (2025). Decolonising Digital Public Infrastructure. Appropriating Technology.

Rwanda Information Society Authority (2025). Rwanda Launches the Center for Digital Public Infrastructure: A New Era of Innovation and Inclusion. Kigali: RISA.

Sanchez Vigueras, R. (2021). Western Africa Regional Digital Integration Program (P176932): Project Information Document (PID). Washington D.C.: World Bank.

Sani, S.S. (2025). Biometrics and digital identity in Africa. Atlantic Council.

Scott, J. C. (1998). Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. Yale University Press.

Sesan, G. and Roberts, T. (2025). Biometric Digital ID in Africa: Progress and Challenges to Date - Ten Country Case Studies. Institute of Development Studies.

Smart Africa. (2025). Transform Africa Summit 2025 – Key Outcomes from the High-Level Panel on Artificial Intelligence (AI), Digital Public Infrastructure (DPI) and Digital Public Goods (DPGs).

Smart Africa. (N.d.). Blueprint for e-Payments for the Facilitation of Digital Trade across Africa.

Smart Africa. (N.d.). Digital Economy Blueprint.

Smart Africa. (N.d.). Digital Identity Blueprint.

Snail ka Mtuze, S. and Musoni, M. (2023). An overview of cybercrime law in South Africa. In: International Cybersecurity Law Review, 4(3), pp. 299-323.

Southern African Development Community (2023). The SADC Digital Transformation Strategy and Action Plan (SADC-DTS). SADC.

Sridharan, S., Narayan, V. and Hardinges, J. (2024). Digital Public Infrastructure: Orientation Matters in Samson, P. and Fay, R. (eds.) The Role of Governance in Unleashing the Value of Data: A CIGI Essay Series, pp. 56 - 60 Centre for International Governance Innovation.

Teevan, C., Pouyé, R. and Kamath, G. (2025). From India Stack to EuroStack: Reconciling approaches to sovereign digital infrastructure. Maastricht: ECDPM, Discussion Paper 384.

Totolo, E. (2025). DPI's Unspoken Trade-Offs: What Leaders Must Weigh to Make Digital Rails Work in Finance and Beyond. Center for Financial Inclusion.

United Nations (N.d.). Global Digital Compact - Revisions. UN.

United Nations (N.d.). Pact for the Future. UN.

United Nations Office for Digital and Emerging Technologies and United Nations Development Programme (2026). The Universal DPI Safeguards Framework is live. UNDP and ODET.

World Bank. (2025). Digital Public Infrastructure and Development: A World Bank Group Approach. WB.

About ECDPM
ECDPM is an independent 'think and do tank' working on international cooperation and development policy.

Since 1986 our staff members provide research and analysis, advice and practical support to policymakers and practitioners across Europe and Africa – to make policies work for sustainable and inclusive global development.

Our main areas of work include:

- EU foreign and development policy
- Migration and mobility
- Digital economy and governance
- AU-EU relations
- Peace, security and resilience
- Democratic governance
- Economic recovery and transformation
- Climate change and green transition
- African economic integration
- Sustainable food systems

For more information please visit www.ecdpm.org

This publication benefits from the structural support by ECDPM's institutional partners: The Netherland, Austria, Belgium, Denmark, Estonia, Finland, Ireland and Luxembourg.

ISSN1571-7577

ecdpm

HEAD OFFICE
SIÈGE
Onze Lieve Vrouweplein 21
6211 HE Maastricht
The Netherlands *Pays Bas*
Tel +31 (0)433 502 900

BRUSSELS OFFICE
BUREAU DE BRUXELLES
Rue Guimard 9, 1040
Brussels *Bruxelles*
Belgium *Belgique*
Tel +31 (0)43 350 29 00

info@ecdpm.org
www.ecdpm.org
KvK 41077447