POLICY BRIEF

Policy Plumbing of Digital Public Infrastructure: Instruments for Effective Implementation

2025

Pierrinne Leukes, Senior Manager, Engagement and Insights, Digital Impact Alliance (South Africa)
Ibrahim Mama Hussein, Senior Manager, Country Engagement, Digital Impact Alliance (Ethiopia)
Ritul Gaur, Policy Advisory, Digital Impact Alliance (India)
Arielle Diamond, Senior Communications Manager, Digital Impact Alliance (Spain)

02

Digital Transformation

Abstract

The rise of digital public infrastructure (DPI) in recent years has brought with it the promise of a more innovative and equitable digital landscape. Globally, nations are increasingly harnessing the benefits of DPI, spurring economic development, fostering greater social and financial inclusion, and enhancing civic engagement – all driven by improved service delivery.

When DPI components – including digital identity, digital payments, and data exchange – are interoperable, modular, extensible, and designed using open tech standards,[1] they can address countless use cases.

Global fora, particularly the G20, have been integral in setting and expanding this agenda. India leveraged its 2023 G20 presidency to build the first-ever multilateral consensus on DPI in recognition of its societal benefits.[2] As the G20 president in 2024, Brazil delivered a joint Declaration on Digital Public Infrastructure, AI and Data for Governance,[3] further recognising DPI as a lever of economic development and highlighting the importance of equitable data governance.

.

.

[1] What is good digital public infrastructure (Digital Impact Alliance)
[2] India's G20 presidency rallied consensus on DPI. Brazil has the opportunity to go even further. (Digital Impact Alliance)
[3] Declaration on Digital Public Infrastructure, AI, and Data for Governance – Joint Communique by the G20 Troika

Diagnosis

This year, with South Africa at the helm of the G20, its agenda is focused on exploring integrated governance to enable digital public infrastructure (DPI) to deliver on its promise. The Digital Economy Working Group has made clear its commitment to "examine the different aspects of policy, regulation, and data governance required for DPI to be transformational".[4] As the first African country to assume the G20 presidency, South Africa's commitment coincides with growing interest in and uptake of DPI across the continent, with many countries taking proactive measures to enhance their enabling infrastructure. Malawi, Uganda, Nigeria, Ghana, Kenya, Sierra Leone, Rwanda, Mauritius, Senegal, and Ethiopia are all early adopters of a DPI approach.

While DPI discourse has traditionally focused on the efficiencies afforded by these systems, today focus is shifting toward the essential work of mitigating potential risks. However, as is often the case, policy innovation lags technological advancements. As DPI advances, policy must keep pace. Drawing lessons from India's experience and Ethiopia's early efforts, we identify best practices for layered policy instruments that support both protection and progress, privacy and flexibility, ensuring DPI delivers on its transformative potential.

Recommendations

While effective DPI implementation requires attention to multiple policy domains, our recommendations focus on three areas:

1. **Equitable data governance frameworks,** including robust consent-based data-sharing architectures and comprehensive data protection

[4] Digital Economic Working Group Issue Note (G20 South Africa)

mechanisms that safeguard individual privacy, ensure responsible data management, and create value for people.

2. **Technical standards**, ensuring the adoption of open protocols and interoperability standards for seamless communication and integration across different systems and platforms.
3. **Institutional oversight mechanisms,** encompassing effective risk management strategies and grievance redressal systems that ensure accountability.

Data governance

Data governance frameworks involve both technical and policy management of the DPI ecosystem, striking a delicate balance between protection and innovation. In India, data governance policy focused on the innovative use of data for economic development.

Four policy instruments guided this approach:

1. The National Data Sharing and Accessibility Policy (2012) established foundational data governance for government datasets, creating classifications for open, registered, and restricted data and defining standards for responsible data sharing between government entities.
2. After the deployment of Aadhaar, India's digital ID, the government introduced the Aadhaar Act (2016) to govern the use of this hyper-sensitive data. The law establishes clear parameters for how biometric and demographic data can be collected, stored, and authenticated.
3. With a focus on empowering data subjects, the eConsent artefact is a digital tool that enables people to determine how their data is used and automates sharing based on their preferences.

4. India's Digital Personal Data Protection Act (2023) regulates the processing of digital personal data to ensure that it is processed lawfully, fairly, and transparently, with explicit consent from individuals.

India's approach was largely innovation-led, using a mix of policy, regulation, and technology to create the foundations for generating maximum value from personal data.

Many African countries have opted to first enact data protection acts, with data governance strategies following later. While 38 African countries have data protection laws, only eight have data strategies.[5] Ethiopia, by contrast, is following India's innovation-led approach, creating its Integrated Data Governance Framework alongside a burgeoning digital ecosystem. This approach enables Ethiopia's data governance strategy to be fit-for-purpose – use case driven and tailored to real needs in health, agriculture, finance, and social protection.

Recommendation: Countries should consider protection and value creation in tandem. This balanced strategy allows for a clearer picture of trade-offs and lends itself to an agile approach to address them.

Technical standards

With data governance frameworks establishing the rules for data usage, the next critical component is implementing technical standards. Technical standards provide the blueprint for how systems interact and exchange data – essential ingredients for DPI to scale effectively.

Three key policies enabled India's successful DPI ecosystem:

[5] Interactive tool: Data policies in African countries (ecdpm)

1. **Open API policies** create standardised methods for systems to communicate seamlessly. Aadhaar's API-first design was a strategic choice to build digital identity to serve multiple use cases. India's Open API Policy (2015) became the technical backbone of its DPI strategy, enabling integration between government and private digital services. This allowed platforms like DigiLocker to interoperate with external systems, creating the environment for a robust digital economy.
2. **Open standards and open-source technologies** ensure systems can work together and help avoid vendor lock-in. India's Policy on Open Standards for e-Governance (2010) mandated platform-neutral standards across all government digital projects.[6] The Policy on Adoption of Open-Source Software (2015) encourages the use of open-source technologies to promote reuse, reduce costs, and foster collaborative innovation. Together, these policies shape a digital ecosystem that is increasingly modular, interoperable, and resilient.
3. **Cybersecurity frameworks** protect digital assets and maintain public trust. India's National Cyber Security Policy (2013) built a secure digital ecosystem through threat prevention frameworks, critical infrastructure protection, and incident response capabilities.

Following India's example, Ethiopia's digital ID system – FAYDA – is built on openness, interoperability, and trust. Through Open API policies, open standards, and open-source technologies, FAYDA enables secure, scalable data exchange across sectors while ensuring sustainability, cost efficiency, and vendor neutrality. These principles allow for easier regional collaboration and interoperability, particularly as Ethiopia aligns with the AU's digital ID interoperability framework. A

[6] E-Governance Policy Initiatives under Digital India (Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India)

robust cybersecurity system, including identity-proofing, encryption, audit logging, and incident response, ensures FAYDA remains secure as usage grows.

Recommendation: Countries should consider developing open standards and open-source policies, establishing API governance that balances openness with security, implementing comprehensive cybersecurity frameworks, and participating in international collaboration on technical standards development.

Institutional oversight

With the policies and technical standards in place to govern data, the next essential ingredient is institutional oversight. Making institutional oversight a reality requires strong institutions with clear mandates and sustainable financing to govern and manage DPI systems.

Three strategies allowed India to build effective institutions:

1. **Pricing policies** for new digital services allow for sustainable funding independent of grants and immune to shifting global priorities. Without them, governments risk unsustainable subsidy costs, service degradation, and long-term financial strain. The Aadhaar (Pricing of Aadhaar Authentication Services) Regulations (2021) established a fee structure that enables cost recovery while maintaining accessibility. A well-designed pricing model secures financial stability that ensures sustainable service maintenance, capacitates enforcement institutions, and encourages private sector collaboration.
2. **Network policies** define the rules of engagement and govern interactions within digital ecosystems. The National Payments Corporation of India (NPCI), which manages the Unified Payments Interface (UPI), exemplifies effective network governance. The NPCI establishes comprehensive rules,

prescribes technical standards, conducts regular compliance audits, sets security protocols, and maintains authority to approve or remove non-compliant actors. This framework strengthens confidence in and the reliability of India's digital payment system.

3. **Grievance redressal** involves addressing complaints from digital service users. India employs multi-layered grievance redressal mechanisms across its DPI systems. While Aadhar deploys multiple channels to process users' issues (such as an online portal and toll-free helpline), UPI-related grievances follow a tiered approach – addressed first through the bank or payment application, and then escalated if unresolved. The Centralised Public Grievance Redress and Monitoring System is a portal connecting citizens to all government departments, enabling formal tracking and resolution of DPI-related issues.

Ethiopia has laid strong policy and technical foundations in support of its DPI ecosystem, but institutional coordination, oversight, and financing must now keep pace. Institutions like the Ministry of Innovation and Technology, the Ethiopian Artificial Intelligence Institute, and the National ID Program are emerging as anchors of DPI governance, but clearer mandates, cross-sector regulatory alignment, and long-term sustainability planning are needed to ensure that DPI systems remain equitable, secure, and accountable as they scale nationally.

Recommendation: Countries adopt context-appropriate pricing and network policies for digital services, ensure robust grievance redressal processes, and invest in well-mandated, accountable institutions to govern DPI with transparency, equity, and resilience.

Conclusion

DPI is more than a set of technologies and systems; it is an approach to their design and governance. When done well, DPI can foster a well-functioning, interconnected digital society. To deliver this impact, the approach must include a holistic policy infrastructure that protects data privacy, ensures data security, expands access to essential services, and generates value for people.

T20 South Africa Convenors

The Institute for Global Dialogue (IGD)

The South African Institute of International Affairs (SAIIA)

The Institute for Pan-African Thought and Conversation (IPATC)

For publication enquiries, please contact t20@t20southafrica.org

Website: www.t20southafrica.org