

State of Internet Freedom in Africa 2026

**The Promise of Digital Public Infrastructure
and the Reality of Its Impact on Human
Rights and Democratic Participation in Africa**

September 2026



Acknowledgements

This report was made possible through the dedication and commitment of many individuals. We extend our heartfelt gratitude to the Editorial Team —Edrine Wanyama, Paul Kimumwe, Dr Peter Mwesige, Raylenne Kambua, Victor Kapiyo and Dr Wairagala Wakabi whose careful review, coordination, and guidance shaped this publication into a coherent and impactful resource.

We also thank the 10 country researchers whose expertise, rigorous analysis, and insights provided the foundation for this year's report. Country Researchers: Ethiopia - Abel Wabella, Kenya - Francis Monyango, Ghana - Felicia Anthonio, Kenya - Francis Monyango, Nigeria - Morisola Alaba, Senegal - Astou Diouf, South Africa - Thomas Linder Tunisia - Yosr Jouini, Uganda - Jackson Leviticus Wandera, Zambia - Richard Mulonga and Zimbabwe - Natasha Msonza

CIPESA deeply appreciates the collective effort that went into producing this edition of the State of Internet in Africa 2026, and we remain inspired by the shared commitment to advancing digital rights and democracy across the continent.

State of Internet Freedom in Africa 2026

The Promise of Digital Public Infrastructure and the Reality of Its Impact on Human Rights and Democratic Participation in Africa

Published September 2026



Creative Commons Attribution 4.0 Licence
<creativecommons.org/licenses/by-nc-nd/4.0>
Some rights reserved.

List of Acronyms and Abbreviations

ACHPR:	African Commission on Human and Peoples' Rights
AfCFTA:	African Continental Free Trade Area
AI:	Artificial Intelligence
API:	Application Programming Interface
ASUTIC:	Association des Utilisateurs des Technologies de l'Information et de la Communication
AU:	African Union
AWS:	Amazon Web Services
BVVK:	Biometric Voter Verification Kit
CIPESA:	Collaboration on International ICT Policy for East and Southern Africa
DIAL:	Digital Impact Alliance
DPI:	Digital Public Infrastructure
DPIA:	Data Protection Impact Assessment
DZAP:	Digital Zambia Acceleration Project
ECOWAS:	Economic Community of West African States
EGDI:	E-Government Development Index
EIU:	Economist Intelligence Unit
EMBs:	Electoral Management Bodies
EQIA:	Equality Impact Assessment
GDP:	Gross Domestic Product
GhIPSS:	Ghana Interbank Payment and Settlement Systems Limited
GSMA:	Global System for Mobile Communications Association
HRBA:	Human Rights-Based Approach
HRIA:	Human Rights Impact Assessment
IDA:	International Development Association
IIDEA:	International Institute for Democracy and Electoral Assistance
IEBC:	Independent Electoral and Boundaries Commission (Kenya)
IEC:	Electoral Commission of South Africa
IGAD:	Intergovernmental Authority on Development
INEC:	Independent National Electoral Commission (Nigeria)
INRIS:	Integrated National Registration Information System (Zambia)
IPRS:	Integrated Population Registration System (Kenya)

IReV:	INEC Result Viewing Portal
ISER:	Initiative for Social and Economic Rights
ITU:	International Telecommunication Union
IUC:	Identifiant Unique du Citoyen (Unique Citizen Identifier - Tunisia)
JICA:	Japan International Cooperation Agency
KIEMS:	Kenya Integrated Election Management System
KRA:	Kenya Revenue Authority
KYC:	Know Your Customer
MOSIP:	Modular Open Source Identity Platform
NDPC:	Nigeria Data Protection Commission
NIA:	National Identification Authority (Ghana)
NIBSS:	Nigeria Inter-Bank Settlement System Plc
NIIMS:	National Integrated Identity Management System (Kenya)
NIMC:	National Identity Management Commission (Nigeria)
NIN:	National Identification Number (Nigeria)
NIRA:	National Identification & Registration Authority (Uganda)
NITA:	National Information Technology Authority
NITA-U:	National Information Technology Authority Uganda
NRC:	National Registration Card (Zambia)
PDPO:	Personal Data Protection Office (Uganda)
POPIA:	Protection of Personal Information Act (South Africa)
POTRAZ:	Postal and Telecommunications Regulatory Authority of Zimbabwe
SIM:	Subscriber Identity Module
UCC:	Uganda Communications Commission
UGHub:	Uganda Government Data Exchange Hub
UN:	United Nations
UNDP:	United Nations Development Programme
UNGPs:	United Nations Guiding Principles on Business and Human Rights
USD:	United States Dollar
VMDs:	Voter Management Devices

Table of Contents

List of Acronyms and Abbreviations	3
Executive Summary	7

1.0 Introduction	11
1.1 Background	11
1.2 Problem	13
1.3 Aims and Objectives	14

2.0 Methodology	15
------------------------	-----------

3.0 Continental Context	16
3.1 Socio-Economic and Democratic Context	16
3.2 Comparative country governance context	18
3.2 Continental Norms and Regional Instruments	20
3.3 Identity as the Primary Layer	19

4.0 Research Findings	21
4.1 Overview of DPI in the Study Countries	21
4.1.1 Digital Identity and Data Exchange Systems	25
4.1.2 Narratives Justifying DPI Deployment	26
4.1.3 Objectives, Priorities and Interests Shaping DPI	28
4.2 Regulatory and Institutional Frameworks Governing DPI in Africa	34
4.2.1 Legal and Regulatory Frameworks Governing DPI	34
4.2.2 Oversight, Accountability, and Institutional Responsibilities	36
4.2.3 Implementation of Safeguards	37
4.2.4 From Legal Safeguards to Practice: Persistent Governance Gaps	38
4.3 Stakeholder Responsibilities on Human Rights across DPI Ecosystems	40
4.3.1 Roles of Private Companies, Donors, and Technology Providers	41
4.3.2 Human Rights Due Diligence in DPI Design and Deployment	43
4.3.4 Accessibility of Grievance and Remedy Mechanisms for Affected Populations	44
4.3.5 Effectiveness of Remedy for Affected Populations	45
4.5 Rights-Respecting, Inclusive, Accountable DPI Governance	47
4.5.1 Reform Priorities	47
4.5.2 Enabling Conditions for Rights-Respecting DPI systems	49
4.5.3 Roles of Stakeholders in Improving DPI Governance	51
4.5.4 Roles of International and Regional Bodies in Establishing Minimum Standards for Rights-Respecting DPI	51

5.0	Impact of DPI on Digital Rights and Democratic Governance	53
	5.1 Equality and Inclusion: Administrative Efficiency as Political Inequality	53
	5.2 Privacy and State Surveillance: interoperability increases state visibility	54
	5.3 Freedom of Expression, Connectivity, and Elections	56
	5.4 Participation and Contestability by Citizens	57
	5.5 Sustained Weaknesses in Accountability and Remedy	58
	5.6 Interoperability Multiplies both Public Value and Systemic Risk	58
	5.7 Digital Sovereignty and Dependence on Vendors and Financiers	59
	5.8 Progress Markers and Areas Needing Change	60
6.0	Conclusion and Recommendations	62
	6.1 Conclusion	62
	6.2 Recommendations	62
	6.2.1 Governments and Public Institutions	63
	6.2.3 Data Protection Authorities, Sector Regulators, and Oversight Institutions	63
	6.2.4 Private Technology Providers, Telecom Operators, Banks, and Payment Firms	64
	6.2.5 Development Partners and DPI Financiers	64
	6.2.6 Civil Society, Media, and Academia	65
	6.2.7 African Union, Regional Economic Communities, and Regional Courts	65

Executive Summary

The 2026 State of Internet Freedom in Africa (SIFA) report examines how Digital Public Infrastructure (DPI) systems are reshaping the relationship between states and citizens, particularly regarding digital rights, democratic governance, and civic participation. Much of the existing work has largely focused on technical design, economic efficiency, and service delivery outcomes, with far less attention to the human rights implications of DPI governance and implementation. This study sought to address this knowledge gap by developing and applying a comparative, human rights-informed assessment framework to examine DPI across 11 African countries: Egypt, Ethiopia, Ghana, Kenya, Nigeria, Senegal, South Africa, Tunisia, Uganda, Zambia and Zimbabwe.

By documenting how DPI deployment is affecting human rights, governance, and democratic participation across 11 countries, this study aims to generate evidence that can support civil society, policymakers, development partners, regional institutions, and technology providers in strengthening rights-respecting DPI governance frameworks before these systems become further entrenched in public administration and everyday life.

Methodologically, the study drew on a Human Rights-Based Approach and an analytical framework informed by Human Rights Impact Assessment to assess DPI systems against internationally recognised human rights standards and emerging global governance principles for digital public infrastructure. More specifically, the study examines DPI as public infrastructure whose benefits and risks depend on law, design, implementation, institutional practice and access to remedy. The study was organised around five main research questions addressing: the systems and political contexts shaping DPI; human rights, inclusion and access to services; legal and institutional safeguards; the distribution of responsibility and accountability; and the conditions required for rights-respecting DPI governance. Within each question, the report identifies the continental pattern and then compares how it appears across the 11 countries.

Findings

The study shows that DPI in Africa is at different stages but moving toward the same functional role of being a reusable key for public and private transactions. The 11 study countries are converging towards more connected identity, payment, data-exchange and service systems, but they differ markedly in scale, sequencing and institutional control. While identity and payments are already mature in several countries, data exchange remains the least developed, least transparent and most unevenly implemented layer.

Governments are giving greater policy weight to digital sovereignty aiming to build local DPI rails, secure data localisation, develop domestic cloud data centres, assert regulatory control over platforms, and reduce dependency on Western or Chinese technology providers. However, in several countries, national DPI architecture remains deeply dependent on external financing, foreign technology providers, and international standards. The World Bank and other development partners, MOSIP, telecom operators, global payment networks and technology vendors remain central in the financing, procurement, development and operation of several DPI systems.

Connectivity has increasingly become a pre-condition for both access to essential services and democratic participation; thus, the shared dependencies mean a cable cut, power failure, cloud outage or internet disruption can interrupt identity, payments and public services together and consequently affect socio-economic and civil-political rights at the same time. For landlocked countries, resilience also depends on neighboring states, border crossings and regional restoration arrangements.

Results also show that countries do not rely on a single law or policy; instead, the legal and institutional framework varies according to the DPI system concerned, with civil registration and identity, telecommunications, digital payments, taxation and other digital public systems operating under their respective sectoral mandates. At the continental level, the study shows that the African Union has also strengthened the policy environment through the 2024 AfCFTA Digital Trade Protocol, African Digital Compact, Continental AI Strategy, and Data Policy Framework. In addition, ratifications of the Malabo Convention had reached 20 by 2 February 2026.

The comparative evidence also shows that there are no overall leaders or laggards. A country can make technical or legal progress in one area and still have serious weaknesses in other areas such as access, oversight or remedy. Nigeria, Ethiopia and Ghana perform strongly on aspects of scale and payments while Kenya and South Africa are comparatively stronger on institutional contestability. The lesson is that advances in one dimension of DPI should not be taken as evidence of progress across the board: technical development, institutional safeguards and rights protection can evolve simultaneously but unevenly and at different speeds within the same country.

Implications on Human Rights and Democracy in Africa

While DPI is often presented as a technical and administrative reform, it has significant implications for human rights, civic participation and democracy in Africa, especially in a context where digital access, institutional capacity, and civic space are uneven. Across the study countries, DPI is being implemented as part of digital transformation initiatives whose record on the continent has prioritised supply-side needs, such as administrative efficiency, at the expense of demand-side outcomes, such as the protection of fundamental rights, including digital inclusion, privacy, freedom of expression and civic participation.

Increased Risk of Digital Exclusion: Integration of DPI systems can reduce transaction costs and improve targeting, but it can also increase the number of services that may become inaccessible when one component of the interconnected system fails. Digitally connected, already documented and urban users tend to realise benefits first while rural residents, low-income users, older people, persons with disabilities, migrants and contested-citizenship communities in countries with weak civil registration records faced greater exclusion. This pattern appears in different forms across all the countries in the sample. For example, in countries such as Kenya and Uganda, the national digital ID systems were criticised for excluding parts of the population, including refugees, stateless persons, and those from rural communities.

Exclusion from Civic Participation: DPI does not necessarily create most underlying inequalities, but it can reproduce or intensify them when unequal documentation, disability, gender, income, geography or language affect the ability to enroll, authenticate or seek correction. These inequalities also determine who can participate safely in digital public life. For example, technology-facilitated gender-based violence (TFGBV), online harassment and misogynistic disinformation can deter women from political and civic participation even where formal digital access is improving.

A voter may be excluded not because an electoral authority made a direct decision, but because a birth, citizenship, address, identity or biometric record held by another agency is missing or wrong. The more services and democratic processes reuse a single foundational record, the more important universal documentation, assisted access and cross-system correction become.

Conclusion

Digital Public Infrastructure is rapidly expanding across Africa. It is effectively galvanising interoperable identity, payment, and data-exchange systems which is equally playing a critical role in shaping the relationship between states and citizens through the opportunities it presents in effective administrative efficiency and financial inclusion. However, these systems are not purely neutral in operations. They have overarching effects on design and governance on the continent. Foundational credentials such as mandatory gateways and access to essential public and private services are increasingly facing flaws in architectural design and utility, technical failures, and inaccurate records. The effect is often a trigger of widespread, cascading exclusion for vulnerable populations, particularly those facing barriers in digital literacy, connectivity, or civil registration such as rural dwellers, women, children and the elderly.

While institutional progress is increasingly visible across the continent, including through recent progressive judicial interventions and regulatory enforcement in countries such as Ghana, Senegal, South Africa, and Uganda, legal and technical capacities remain uneven, and in many cases, inadequate. Technical integration is progressing much faster than institutional frameworks which are required for effective governance. The effect as shown in the study findings is fragmented oversight, opaque and poor data-sharing practices, and limited public verifiability. Furthermore, the convergence of foundational identity systems with the work of election management bodies (EMBs) and democratic processes and the telecommunications infrastructure has exposed citizens to severe democratic risks, where network disruptions and administrative flaws lead to impairment of political participation and protection and enjoyment of civic freedoms.

Ultimately, prolonged legitimacy and trust of African DPI largely depend on the establishment and integration of robust, rights-respecting safeguards into the system functioning lifestyle rather than treating them as retroactive compliance measures. Ensuring a resilient, functional and inclusive digital future requires maintaining accessible non-digital channels, enforcing data protection principles and rights with strictness placed on purpose and data minimization, ensuring independent institutional oversight, ensuring open connectivity in democratic seasons and political transitions, and providing timely, fair enforceable avenues for access to legal remedy

Recommendations

Governments - Executive

- Establish robust governance frameworks for rights-respecting DPI through appropriate national policies, laws, strategies and action plans, while investing in complementary infrastructure, affordable connectivity, local innovation and institutional capacity and skills.
- Require public human rights, data protection and equality impact assessments before major DPI systems are deployed or significantly expanded, with particular attention to exclusion, discrimination, surveillance, cybersecurity, function creep and access to remedy.
- Ensure transparency, accountability and meaningful alternatives in DPI implementation by publishing information in legal mandates, responsible agencies, key suppliers/financiers, and system performance, and providing accessible correction, complaint procedures, and non-digital fallback mechanisms.
- Protect democratic participation from technology-related restrictions and risks by ending internet shutdowns and subjective DPI, automated systems and other technologies used in elections to independent scrutiny, appropriate safeguards and effective remedy.

Oversight Bodies

- Strengthen proactive and coordinated oversight of DPI through regular audits of national identity databases, interoperability platforms, and government-to-person payment systems.
- Safeguard the independence, capacity and transparency of oversight institutions through adequate resourcing, transparent appointments, effective investigative powers and regular public reporting on enforcement and system performance.
- Embed privacy, security, transparency and remedy in DPI-related products and services through data minimisation, purpose limitation, robust access controls, appropriate contractual transparency, and effective mechanisms for addressing harm.

Private Technology Providers, Telecom Operators, Banks, and Payment Firms

- Conduct and disclose UNGP-aligned human-rights due diligence for high-risk DPI such as identity, biometric, data-exchange and surveillance contracts, including risks created by downstream use by government and other public bodies.
- Embed privacy, security, transparency and remedy in DPI-related products and services through data minimisation, purpose limitation, robust access controls, appropriate contractual transparency and effective mechanisms for addressing harm.

Development Partners and DPI Financiers

- Link financing and scale-up to demonstrate inclusion, rights protection, effective oversight, and access to remedy, rather than measuring success primarily through enrolment, infrastructure coverage, or transaction volumes.
- Support independent technical, human-rights, and accessibility audits that are published before mandatory-use rules are expanded.
- Strengthen the long-term capacity and independence of domestic regulators, courts, civil society, and complaint systems rather than building project-specific safeguards that disappear when financing ends.
- Invest in open-access, resilient and route-diverse, energy- and climate-resilient infrastructure alongside DPI.

Civil Society, Media, and Academia

- Move DPI scrutiny upstream by engaging in policy, procurement, design and impact-assessment processes before systems are deployed, while continuing investigation, public interest reporting, and strategic litigation where necessary.
- Strengthen evidence and capacity to scrutinise the human and technical impacts of DPI, including exclusion, surveillance, identity and authentication failures, automated decision-making, vendor arrangements, and harms disproportionately affecting marginalised groups. .
- Build civil-society and media capacity to scrutinise less visible infrastructure: identity-to-election APIs, access logs, vendor and hosting arrangements, automated matching, recommender systems and AI-assisted election tools.

Regional Bodies: African Union, Regional Economic Communities, and Regional Courts

- Rely on the African Charter, the Malabo Convention, the AU Data Policy Framework, the African Digital Compact, the AfCFTA Protocol on Digital Trade, and the Universal DPI Safeguards Framework to develop minimum rights-respecting DPI standards.
- Operationalise ACHPR Resolution 580 (2024) together with Resolution 655 (2026) through systematic election observation, public reporting, and follow-up when states order shutdowns or platform restrictions; incorporate assessment of EMB independence, digital violence, disinformation responses, and access to effective redress.
- Develop regional resilience standards and cross-border restoration protocols for infrastructure carrying DPI, including outage reporting, open-access corridors, and continuity arrangements for landlocked states. Promote portable workloads, open standards, and shared technical capacity so national systems do not depend on the same small supplier set.
- Develop regional guidance for election-related use of foundational digital identity, building on the AU Interoperability Framework for Digital ID.

1.0 Introduction

1.1 Background

Digital Public Infrastructure (DPI) refers to reusable foundational systems such as digital identity, payments and data exchange that enable participation in the digital economy, access to services and interaction. Africa is in the middle of a foundational digital transformation that is increasingly shaping how public authority is exercised, how government services are delivered, how citizens prove their identity, and how essential public and private services are accessed. Governments are rapidly consolidating fragmented, legacy e-government portals into interconnected DPI. DPI are the shared, interoperable digital systems or rails that underpin government-to-citizen interactions, and they are built around three foundational pillars: digital identity, digital payments systems, and data exchange platforms.¹

The DPI approach is essentially characterized by three main concepts: common design philosophy that emphasises interoperability, extensibility, protocol-based systems and data federation; robust governance that directs DPI to be people-centric to safeguard users' rights to privacy and autonomy; and market or private sector participation while ensuring a competitive market and incentives alignment to avoid market capture by powerful players.

The infrastructure shift is being driven by strong domestic and international momentum. Across the continent, siloed government systems are being replaced with more interconnected digital systems that can facilitate secure data exchange that enables identity verification, cross-border payments, and access to essential socio-economic services.² By the end of September 2026, 17 African countries were among the 39 global participants in the multilateral 50-in-5 campaign aimed at helping countries design, launch, and scale components of their digital public infrastructure.³ Early success of DPI components in countries such as Ethiopia, Ghana, Kenya, Nigeria, Rwanda, Togo and Uganda, coupled with continental aspirations for digital transformation and trade,⁴ and various donor-driven initiatives such as those by the World Bank, UNDP and the Gates Foundation, have amplified the impetus for DPI adoption.⁵

¹ Carnegie Endowment for International Peace. (2025). Digital Public Infrastructure: A Practical Approach for Africa. <https://carnegieendowment.org/research/2025/02/digital-public-infrastructure-a-practical-approach-for-africa>

² Africa should invest in Digital Public Infrastructure to aid regional integration <https://blogs.lse.ac.uk/africaatlse/2026/03/17/africa-should-invest-in-digital-public-infrastructure-to-aid-regional-integration/>; Bridges or Barriers? Governing Africa's Digital Public Infrastructure <https://www.thedatasphere.org/news/governing-africa-digital-public-infrastructure/>

³ Implementing digital public infrastructure, safely and inclusively, 50-in-5, <https://50in5.net/#about>

⁴ Digital Transformation Strategy for Africa 2020-2030 <https://www.studocu.com/row/document/universite-chretienne-bilingue-du-congo/gestion-de-projet/digital-transformation-strategy-for-africa-2020-2030-vision-objectives/135319883>; Smart Africa Blueprints <https://smartafrica.org/blueprint/>

⁵ Global Digital Public Infrastructure Program: From Foundations to Scale <https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program>; Digital Public Infrastructure (DPI) <https://www.undp.org/digital/digital-public-infrastructure>; Digital Public Infrastructure <https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/digital-public-infrastructure>

Proponents frame DPI as a prerequisite for accelerating economic growth, improving public service delivery, administrative efficiency, tax mobilisation, financial inclusion, social protection and regional digital integration. It is estimated that increasing full digital ID coverage could unlock between 3 and 13% of GDP across developing economies by 2030.⁶ Notably, at least 44 countries on the continent have developed data protection laws that offer promising rights-respecting frameworks for regulating the collection and processing of personal data. However, the maturity of data protection authorities and frameworks remains uneven. In 2026, the scale of DPI is projected to grow rapidly across the continent. By the end of 2025, at least 49 African countries operated some form of biometric identification systems, which are central to managing identity, elections, border control, and SIM card registration.⁷ Digital identity is growing, with Nigeria leading with 136 million National Identification Number (NIN) enrollments;⁸ followed by Ethiopia with 50 million,⁹ and Ghana with 20 million.¹⁰ Similar programmes are expanding in Kenya, South Africa and Uganda. Digital payments are the most advanced DPI pillar on the continent given the widespread mobile money adoption, although maturity levels vary by country. There were at least 36 live instant payment rails across 31 countries processing nearly USD 2 trillion across 64 billion transactions annually in 2024.¹¹ Data exchange remains nascent, with promising developments in Ghana and Uganda following the establishment of the Ghana Interbank Payment and Settlement Systems Limited (GhIPSS) in 2007, which laid the foundational framework for all financial data exchange in the country, and the launch of Uganda's open-source platform, UGHub, which was designed for data and systems integration.¹²

The expansion of DPI is occurring alongside a maturing continental normative framework. The African Union (AU) has adopted the Digital Transformation Strategy for Africa (2020–2030), the AU Data Policy Framework (2022), the AfCFTA Protocol on Digital Trade (2024), and the African Digital Compact (2024). Furthermore, the African Commission on Human and Peoples' Rights (ACHPR) adopted the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019,¹³ and various resolutions such as Resolution 362 on online expression,¹⁴ Resolution 630 on information integrity,¹⁵ 631 on digital content,¹⁶ Resolution 580 on internet shutdowns,¹⁷ Resolution 655 on elections and digital rights,¹⁸ alongside global standards such as the UN Universal DPI Safeguards Framework¹⁹ and the UN Guiding Principles on Business and Human Rights.²⁰

6 Africa's Biometric Market: Strategic but Lacking Local Leaders <https://www.ecofinagency.com/news-digital/1402-52910-africa-s-biometric-market-strategic-but-lacking-local-leaders>

7 Africa's Biometric Market: Strategic but Lacking Local Leaders <https://www.ecofinagency.com/news-digital/1402-52910-africa-s-biometric-market-strategic-but-lacking-local-leaders>

8 The Guardian Newspaper, (2026, July 7). 136m Nigerians get NIN as NIMC's new act takes effect <https://guardian.ng/featured/136m-nigerians-get-nin-as-nimcs-new-act-takes-effect/>

9 Kana TV News, What Is FaydaVerse? The Ethiopian National ID Program That Became a Company (2026), <https://kanatelevision.com/news/what-is-faydaverse-the-ethiopian-national-id-program-that-became-a-company-and-how-it-plans-to/>

10 National Identification Authority. (2026, August 17). Registration Statistics. <https://nia.gov.gh/nia-registration-statistics/>

11 AfricaNenda Foundation. (2025). SIIPS 2025: State of Inclusive Instant Payment Systems in Africa. <https://africanenda.org/siips/siips-report-2025>

12 Carnegie Endowment for International Peace. (2025). Digital Public Infrastructure: A Practical Approach for Africa. <https://carnegieendowment.org/research/2025/02/digital-public-infrastructure-a-practical-approach-for-africa>

13 ACHPR, Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 <https://achpr.au.int/en/node/902>

14 Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res.362(LIX)2016 <https://achpr.au.int/en/adopted-resolutions/362-resolution-right-freedom-information-and-expression-internet>

15 Resolution on developing Guidelines to assist States monitor technology companies in respect of their duty to maintain information integrity through independent fact checking - ACHPR/Res.630 (LXXXII) 2025 <https://achpr.au.int/en/adopted-resolutions/achprres630-lxxxii-2025>

16 Resolution on working towards the assessment of public interest content in this digital era and developing guidelines to ensure a public interest element for all platforms operating in Africa - ACHPR/Res.631 (LXXXII) 2025 <https://achpr.au.int/en/adopted-resolutions/631-achprres631-lxxxii-2025>

17 Resolution on Internet Shutdowns and Elections in Africa - ACHPR/Res.580 (LXXVIII)2024 <https://achpr.au.int/en/adopted-resolutions/580-internet-shutdowns-elections-africa-achprres580-lxxviii>

18 Resolution on Elections in Africa in 2026 - ACHPR/Res.655(LXXXVI) 2026 <https://achpr.au.int/en/adopted-resolutions/achprres655lxxxvi-2026>

19 UNDP. (2024). Universal DPI Safeguards Framework: A guide to building safe and inclusive DPI for societies (updated 2025). <https://www.undp.org/publications/universal-safeguards-digital-public-infrastructure>

20 Office of the United Nations High Commissioner for Human Rights. (2011). Guiding principles on business and human rights. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

1.2 Problem Statement

While DPI is often presented as a technical and administrative reform, it has significant implications for privacy, inclusion, equality, accountability, and democratic participation, particularly in contexts where digital access, institutional capacity, and civic space are uneven. DPI is being implemented as part of digital transformation initiatives whose record on the continent has prioritised supply-side needs, such as administrative efficiency, over demand-side outcomes, such as the protection of fundamental rights. This is crucial, especially in a context where 540 million Africans lack a foundational legal identity document, which locks out key groups, including women and other marginalised groups such as persons with disabilities and older persons, from essential services, financial systems and the broader digital economy.²¹ In Kenya and Uganda, the national digital ID systems were criticised for excluding parts of the population, including refugees, stateless persons, and those from rural communities.²² Moreover, civil society organisations have raised concerns about their exclusion from the design, governance, and oversight of DPI across Africa.²³ Other constraints to DPI, which underlie other digital transformation initiatives, include a lack of robust DPI legal and regulatory frameworks, low digital literacy, donor dependence, vendor lock-in, and limited digital access and infrastructure. Media coverage of DPI is also limited, potentially hindering public awareness and understanding of the subject.²⁴

More concerningly, digital transformation across the continent is unfolding within a highly precarious environment for digital rights and democratic participation. Digital systems are being rapidly deployed in environments where civic space is shrinking, digital rights are being restricted, democracy is being strangled, and trust between citizens and governments is waning.²⁵ Without stringent enforcement of human rights safeguards, meaningful public engagement, robust independent oversight, or necessary transparency and accountability mechanisms, the DPI pillars remain vulnerable to abuse by autocratic regimes determined to undermine democracy, expand state surveillance, perpetuate systemic marginalisation, and entrench digital authoritarianism.²⁶

As African countries transition from their fragmented legacy digital systems into deeply interconnected digital public ecosystems, the foundations being laid to build them today will ultimately shape the future of digital rights, internet freedom and democratic governance. A critical governance challenge is that state and market capacity to deploy data-intensive digital infrastructure is expanding significantly faster than the institutional capacity to constrain its power, protect fundamental rights, or provide accessible remedy. While DPI is often presented as a neutral, technical upgrade to public administration, in practice, it functions as a rights and power amplifier. This is because when digital identity, payments, and data exchange are linked, the authority to verify identity or process data can easily become the authority to grant or deny rights.

Despite growing investments in DPI across Africa, limited research has examined how these systems are reshaping the relationship between states and citizens, particularly regarding digital rights, democratic governance, and civic participation. Existing work has largely focused on technical design, economic efficiency, and service delivery outcomes, with far less attention to the human rights implications of DPI governance and implementation.

²¹ Invisible No More: Securing Legal Identity as a Human Right <https://saiia.org.za/research/invisible-no-more-securing-legal-identity-as-a-human-right/>; Why women lack ID — and what policymakers can do <https://www.womensworldbanking.org/insights/why-women-lack-id-and-what-policymakers-can-do/>

²² Bridges or Barriers? Governing Africa's Digital Public Infrastructure <https://www.thedatasphere.org/news/governing-africa-digital-public-infrastructure/>

²³ The People's Network: Civil Society Organizations in Digital Public Infrastructure Development in Africa https://dial.global/wp-content/uploads/2025/10/CSOs_DPI_Engagement_Final.pdf

²⁴ Media Coverage of Digital Public Infrastructure and Digital Public Goods in Eastern Africa https://cipesa.org/wp-content/files/documents/Executive_summary_DPI.pdf

²⁵ State of Internet Freedom in Africa 2023 A Decade of Internet Freedom in Africa Recounting the Past, Shaping Internet the Future https://cipesa.org/wp-content/files/reports/SIFA23_Report.pdf; State of Internet Freedom in Africa 2024 Africa's Electoral Democracy and Technology: Pitfalls and Promises https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf

²⁶ Digital Public Infrastructure in Africa: A Looming Crisis of Equitable Access, Digital Rights, and Sovereign Control <https://cipesa.org/2025/07/digital-public-infrastructure-in-africa-a-looming-crisis-of-equitable-access-digital-rights-and-sovereign-control/>

1.3 Aims and Objectives

This study sought to explore the critical tension between the promise of DPI and its risks and impact on digital rights, internet freedom and democratic governance. It focuses on 11 countries: Egypt, Ethiopia, Ghana, Kenya, Nigeria, Senegal, South Africa, Tunisia, Uganda, Zambia and Zimbabwe.

To address this gap, the study developed and applied a comparative, human rights-informed framework to examine DPI across selected countries. Drawing on a Human Rights-Based Approach and an analytical framework informed by Human Rights Impact Assessment (HRIA), it assessed DPI systems against internationally recognised human rights standards and emerging global governance principles for digital public infrastructure. By examining how DPI deployment affects human rights, governance, and democratic participation across the 11 countries, this study generates evidence to support civil society, policymakers, development partners, regional institutions, and technology providers in strengthening rights-respecting DPI governance frameworks before these systems become further entrenched in public administration and everyday life.

2.0 Methodology

This study applied a Human Rights-Based Approach (HRBA), informed by Human Rights Impact Assessment principles, the UN Universal Digital Public Infrastructure Safeguards Framework and the UN Guiding Principles on Business and Human Rights.²⁷ The study examines DPI as public infrastructure whose benefits and risks depend on law, design, implementation, institutional practice and access to remedy. The analysis is organised around five main research questions addressing: the systems and political contexts shaping DPI; human rights, inclusion and access to services; legal and institutional safeguards; the distribution of responsibility and accountability; and the conditions required for rights-respecting DPI governance. Within each question, the report identifies the continental pattern and then compares how it appears across the 11 countries.

The evidence combines country-level fieldwork and documentary research with comparative desk research. It includes a review of legislation, regulations, court decisions, government and regulator publications, programme documents, civil-society and media reporting and, in several countries, interviews or stakeholder evidence.

The comparative analysis focuses on how digital identity, payment or data-exchange systems affect access to services, information, participation, and accountability. Democratic governance is assessed through participation, public contestability, institutional independence, transparency, judicial and regulatory checks, civic space, and access to remedy. The 11 countries are treated as case studies rather than a statistically representative sample of Africa. They nevertheless capture different political systems, regions, levels of connectivity, stages of DPI development and institutional arrangements. Comparisons are therefore used to identify recurring mechanisms and contrasting choices, not to estimate continental prevalence from the sample.

Election technology is used as an example within this framework and is not treated as synonymous with DPI, and includes the digital systems used across the electoral cycle, including voter registration, voter identification, results transmission and public information systems. Election-related DPI describes the point at which a foundational identity, population register, data-exchange service or connectivity layer materially determines electoral inclusion, administration or integrity. This distinction matters because the two domains are increasingly converging while remaining governed by different mandates, laws and accountability institutions.

The availability of public information on DPI varies considerably across the 11 countries. Several DPI systems remain pilots or are changing institutional form. There is inconsistent information in the public domain on procurement, data access logs, error rates, correction times, data protection, equality or human-rights impact assessments, and grievance outcomes, vendor contracts, and vendor or project-specific corporate human-rights due diligence. The report does not treat absence of public evidence as proof that an internal process or safeguard does not exist.

27

UNDP. (2026). How the DPG Standard and Universal DPI Safeguards Framework are charting a safe and inclusive digital future. <https://www.undp.org/digital/blog/how-dpg-standard-and-universal-dpi-safeguards-framework-are-charting-safe-and-inclusive-digital-future>; UNDP. (2024). Universal DPI Safeguards Framework: A guide to building safe and inclusive DPI for societies (updated 2025). <https://www.undp.org/publications/universal-safeguards-digital-public-infrastructure>; Office of the United Nations High Commissioner for Human Rights. (2011). Guiding principles on business and human rights. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

3.0 Continental Context

Africa is moving from stand-alone and siloed digitisation and department-specific e-government portals towards interconnected DPI, comprising reusable foundational digital identity, instant payment systems and data-exchange. Across the study countries, the three layers are evolving at different speeds, shaped by national development priorities and strategies, regional integration goals, development partners and global initiatives such as the 50-in-5 campaign.

This technical expansion is occurring within an uneven governance landscape, unequal digital access and contested civic space. Although at least 44 African countries have enacted personal data protection laws, enforcement, regulatory independence and judicial remedy vary. The International Telecommunication Union (ITU) estimated that 38% of Africa’s population used the internet in 2024, compared with 57% in urban areas and 23% in rural areas.²⁸ Access Now documented 30 internet shutdowns in 15 African countries in 2025.²⁹ In 2026, two elections-related internet shutdowns were documented in Uganda and the Democratic Republic of Congo.³⁰ While trends in internet shutdowns vary across the study countries, government control over connectivity remains a recurring democratic risk and an obstacle to the effective functioning of DPI.

Election administration forms part of this wider digital environment. Across Africa, biometric registration and electronic voter identification are common undertakings by election management bodies (EMBs), but paper ballots and human-readable result records remain central to verifiability and continuity. The recurring governance problem is not digitisation itself; it is the combination of technically complex systems, unequal connectivity, vendor dependence and weakly specified exception or audit rules. International IDEA cautions that biometrics can improve duplicate detection and authentication but do not substitute for sound electoral governance.³¹

3.1 Socio-Economic and Democratic Context

Evaluating DPI in Africa requires situating national progress within global benchmarks and continental baselines. As shown in the table below, globally, digital transformation is advancing rapidly. Global internet penetration stands at 67.0%, average UN E-Government Development Index (EGDI) scores hover at 0.6382, and human development averages 0.739 (UNDP). In contrast, Africa remains the lowest-scoring region globally across key digital maturity indices, with a continental average internet penetration of 38.0%, an average EGDI score of 0.4247, an average sub-Saharan HDI score of 0.549, and an average EIU Democracy Index score of 4.04 out of 10.

Table 1: Key Socio-Economic & Digital Indicators

28 International Telecommunication Union. (2025). Measuring digital development: Africa. https://www.itu.int/itu-d/reports/statistics/wp-content/uploads/sites/5/2025/04/2500037E_SDDT_2025_Africa_FINAL.pdf

29 Access Now / #KeepItOn. (2026, March 31). Internet shutdowns in Africa in 2025. <https://www.accessnow.org/press-release/resilience-and-resistance-in-internet-shutdowns-in-africa-in-2025/>

30 Access Now / #KeepItOn. (2026). 2026 elections and internet shutdowns watch. <https://www.accessnow.org/campaign/2026-elections-and-internet-shutdowns-watch/>

31 International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections?lang=en>

Country	Population	Mobile Connections and (Penetration %)	Internet Users and (Penetration %)	GDP (Per Capita) PPP USD	Country HDI Score (Ranking)	EGDI Score	EIU Democracy Score
Egypt	112M	121M (102%)	96.3 (81.9%)	23,321	0.754 (100)	0.6699 (87th)	2.79 (Authoritarian)
Ethiopia	126M	93.2M (68.4%)	29.5M (24%)	4,740	0.497 (180)	0.4100 (158th)	3.00 (Authoritarian)
Ghana	34M	41.8M (119%)	26.3M (74.6%)	3,257	0.628 (143)	0.6800 (82nd)	6.30 (Flawed Democracy)
Kenya	55M	68.8M (121%)	27.4M (40.5%)	7,930	0.628 (152)	0.6314 (109th)	5.05 (Hybrid Regime)
Nigeria	220M	182.2M (84.1%)	109M (45.5%)	9,488	0.560 (161)	0.5200 (138th)	4.23 (Hybrid Regime)
Senegal	18M	22.7M (121%)	11.3M (60.6%)	4,496	0.530 (169)	0.5163 (135th)	6.48 (Flawed Democracy)
South Africa	60M	124M (193%)	50.8M (78.9%)	13,599	0.741	0.7300 (65th)	7.05 (Flawed Democracy)
Tunisia	12M	10.8M (89.9%)	9.3M (77.7%)	4,350	0.746 (105)	0.6935 (87th)	4.65 (Hybrid / Auth.)
Uganda	48M	47.1M (100%)	18.5M (38.4%)	3,276	0.582 (157)	0.4800 (150th)	3.55 (Authoritarian)
Zambia	20M	26.2M (92.1%)	7.1M (33%)	4,570	0.595 (153)	0.4700 (152nd)	5.40 (Hybrid Regime)
Zimbabwe	16M	16.8M (107%)	6.54M (38.4%)	8,443	0.598 (146)	0.4200 (156th)	3.04 (Authoritarian)
Africa		87%	38%	4,800	0.549	0.4247	4.04
Global		110%	67%	23,500	0.739	0.6382	5.23

Across the study countries, there is significant asymmetry. Egypt, Ghana, South Africa, and Tunisia possess digital architectures and e-government scores that exceed both the African regional baseline and the global average. South Africa leads the continent on the UN EGDI with a score of 0.7300 (ranked 65th globally), supported by an internet penetration rate of 78.9% (50.8 million users), mobile penetration of 193.0%, a “High” HDI score of 0.741 (nearing the global average of 0.739), and a “Flawed Democracy” EIU rating of 7.05. Egypt combines high digital penetration of 81.9% internet penetration (96.3 million users) and 102.0% mobile penetration, an EGDI score of 0.6699 (ranked 87th), a GDP per capita (PPP) of USD 23,321 (matching the global average), and an HDI score of 0.754, though operating within an “Authoritarian” EIU Democracy score of 2.79.

The mid-tier countries are Kenya, Nigeria, Senegal, and Zambia which exceed the African regional baseline for connectivity and e-government, but trail global internet access averages (67%) due to significant demand-side constraints, such as device costs, digital literacy, and rural infrastructure gaps. The laggards are Ethiopia, Uganda, and Zimbabwe, which are characterised by EGDI scores near or below the African regional baseline (0.4247), low internet penetration, and restrictive democratic environments that create acute risks of digital and institutional exclusion.

A comparison of the dataset demonstrates that technical e-government maturity (EGDI) and high mobile penetration do not automatically correlate with democratic governance or human rights safeguards. Countries like Egypt (EGDI 0.6699) and Ethiopia (EGDI 0.4100) demonstrate advanced state digital capability and expansion or state-led scale while operating within restrictive “authoritarian” environments (EIU scores < 3.25). Conversely, countries like Kenya, Ghana, and South Africa pair high/mid-tier digital capabilities with judicial review and are rated as “Flawed Democracy” or “Hybrid” systems, highlighting that human rights safeguards depend on institutional independence and civic contestability rather than technical maturity.

3.2 Comparative Country Governance Context

The strongest comparative divide is between the pace of digital integration and the capacity of institutions to govern it, rather than between regions. Several countries have made rapid technical progress, but human rights safeguards, correction routes and public accountability remain uneven.

Across Africa, the same divergence is visible between expanding digital state capacity and the institutions that constrain its use. More services, identities and payments are becoming digitally connected, while courts, regulators, election-management bodies, legislatures and civil society have very different levels of independence and technical capacity. The result is that similar infrastructure can support inclusion in one setting and deepen exclusion or state visibility in another.³²

North Africa illustrates how legal and technical change can move in different directions. In Egypt, the Digital Egypt platform offered 242 government services by 21 July 2026, with the Ministry of Communications and Information Technology targeting more than 270 by the end of the year.³³ The Central Bank of Egypt had also begun demonstrating remote customer identification through the Haweya Digital Financial Identity platform by November 2025.³⁴ Egypt's Personal Data Protection Law No. 151 of 2020 only became operational on 2 November, 2025 through Executive Regulations No. 816 of 2025, which improved the legal environment, but the independence and practical authority of the Personal Data Protection Center will be tested during implementation.³⁵ Tunisia combines a Unique Citizen Identifier created by Decree-Law No. 2020-17, the e-Houwiya Mobile ID service, and a 2024 law enabling a new biometric national identity card.³⁶ From 1 July 2026, Mobile ID also became mandatory for approved online project declarations, showing how a credential introduced as voluntary can become a compulsory one service at a time.³⁷ These changes are taking place while civic space has tightened.³⁸

East Africa contains three different versions of the same tension. Ethiopia is scaling Fayda rapidly. Ethio Telecom reported in August 2026 that it had registered nearly 32 million (69 per cent of the total national population) people since joining the programme on 24 April 2024, and the identity programme itself was re-established on 4 August 2026 as Faydaverse.³⁹ Kenya is introducing Maisha Namba into an already mature eCitizen and mobile-money environment, and the programme has repeatedly been tested in court.⁴⁰ Uganda has an operational National Identification Register and UGHub data exchange. NITA-U reports more than 135 entities on UGHub, and the National Identification & Registration Authority (NIRA) restarted mass enrolment and

³² Digital Impact Alliance. (2025, October 9). The people's network: Civil society organizations in DPI development in Africa. <https://dial.global/research/civil-society-dpi-africa/>; International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/publications/catalogue/html/case-democracy-stack-rethinking-digital-public-infrastructure>

³³ State Information Service, Egypt. (2026, July 21). Communications Minister: Egypt to offer more than 270 digital government services by end-2026. <https://sis.gov.eg/en/media-center/news/communications-minister-egypt-to-offer-more-than-270-digital-government-services-by-end-2026/>

³⁴ Central Bank of Egypt. (2025, November 16). PAFIX 2025: Digital Financial Identity platform (Haweya). <https://www.cbe.org.eg/en/news-publications/news/2025/11/16/18/47/paper-centfix-2025>

³⁵ Personal Data Protection Center, Egypt. (2026). Legal framework: Personal Data Protection Law No. 151 of 2020 and Executive Regulations No. 816 of 2025. <https://www.pdpc.gov.eg/>; Shand Partners. (2026, January 11). Executive regulations of the data protection law in Egypt (Law No. 151 of 2020). <https://www.shand-partners.com/insights/briefings/telecoms-media-technology/the-issuance-of-the-executive-regulations-of-the-data-protection-law-and-the-establishment-of-the-data-protection-centre/>

³⁶ Ministry of Communication Technologies, Tunisia. (n.d.). e-Houwiya / Mobile ID. Retrieved September 13, 2026, from <https://www.mobile-id.tn/accueil>; Tunisia Legal Database / DCAF. (2024, March 11). Organic Law No. 2024-22 amending Law No. 93-27 on the National Identity Card. <https://legislation-securite.tn/latest-laws/loi-organique-n-2024-22-du-11-mars-2024-modifiant-et-completant-la-loi-n-93-27-du-22-mars-1993-relative-a-la-carte-nationale-didentite/>; Tunisia Legal Database / DCAF. (2020, May 12). Decree-Law No. 2020-17 on the Unique Citizen Identifier. <https://legislation-securite.tn/latest-laws/decret-loi-du-chef-du-gouvernement-n-2020-17-du-12-mai-2020-relatif-a-lidentifiant-unique-du-citoyen/>

³⁷ Tunis Afrique Presse / Tunisian Investment Authority. (2026, June 24). "Mobile ID" mandatory for project declarations from 1 July 2026. <https://www.tap.info.tn/en/Portal-Economy/20326511-mobile-id>

³⁸ Human Rights Watch. (2026, September 2). Tunisia: Civil society under siege. <https://www.hrw.org/news/2026/09/02/tunisia-civil-society-under-siege>

³⁹ Ethiopian Investment Holdings. (2026, August 4). National ID Program reestablished as state-owned enterprise "Faydaverse" to anchor nationwide digital public infrastructure. <https://eih.et/national-id-program-reestablished-as-state-owned-enterprise-faydaverse-to-anchor-nationwide-digital-public-infrastructure-and-joins-ethiopian-investment-holdings-portfolio/>; Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethio-telecom.et/2025-26-budget-year-annual-business-performance-report/5/>

⁴⁰ High Court of Kenya at Garissa. (2025, January 21). Haki na Sheria Initiative & 3 others v. Attorney General & 4 others (Petition E008 of 2021) [2025] KEHC 221 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2025/221/eng@2025-01-21>; Directorate of Immigration Services, Kenya. (2024, September 19). Issuance of Maisha Card IDs. <https://immigration.go.ke/issuance-of-maisha-card-ids/>; High Court of Kenya. (2020, January 30). Nubian Rights Forum & 2 others v. Attorney General & 6 others; Child Welfare Society & 8 others (Interested Parties) (Petition 56, 58 & 59 of 2019, Consolidated) [2020] KEHC 8772 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2020/8772>

renewal on 15 May 2025.⁴¹ Yet the 10 June 2025 dismissal of the national-ID exclusion challenge and the Uganda Communications Commission's (UCC) 13–18 January 2026 election-period internet restriction show that access and political contestability remain uneven.⁴² In some domains, technical integration is advancing faster than safeguards.

West Africa shows stronger payment integration alongside divergent accountability paths. Ghana combines the Ghana Card with mature payment infrastructure. The Ghana Interbank Payment and Settlement Systems Limited (GhIPSS) processed 530 million transactions worth GHS 1.73 trillion in 2025. The Supreme Court added an important precedent on privacy in *Gorni v Vodafone Ghana Ltd and Others* on 25 February 2026 when it held that the unauthorised linking of a SIM and mobile-money account to an individual's Ghana Card details breached constitutional privacy and attracted damages.⁴³ In Nigeria, the National Identification Number (NIN) enrollment now stands at 136 million.⁴⁴ Through Nigeria Inter-Bank Settlement System (NIBSS), it also launched the National Payment Stack on 23 June 2025, while the National Identity Management Commission Act, 2026 further strengthened identity-database harmonisation.⁴⁵ Senegal is accelerating interoperability under the New Deal Technologique.⁴⁶ On 16 January 2026, the Ministry of Communication, Telecommunications and the Digital Economy described a JICA-supported inter-ministerial data-exchange project based on common, secure infrastructure.⁴⁷ The ECOWAS Court's 14 May 2025 judgement against the 2023 internet shutdowns provides a significant regional route for accountability.⁴⁸ The regional pattern is therefore not simply more DPI, but more DPI combined with different institutional routes for challenge and remedy.

Southern Africa is similarly mixed. South Africa is building a functional Digital ID and MzansiXchange on top of the National Population Register and Smart ID system, with a phased 2025–2030 roadmap and an independent Information Regulator operating alongside the programme.⁴⁹ Zambia is expanding digital identity, e-government and payment infrastructure under the Digital Zambia Acceleration Project, for which the World Bank approved a US\$100 million IDA grant in September 2025.⁵⁰ The country maintained open connectivity during the 13 August 2026 election,⁵¹ although the Cyber Security Act No. 3 of 2025 increases the importance of independent oversight of interception powers.⁵² Zimbabwe remains more incremental and sectoral, but the National Artificial Intelligence Strategy 2026–2030, formally launched in March 2026, envisages a National AI and Data

-
- 41 National Information Technology Authority–Uganda (NITA-U) <https://x.com/NITAUGanda1/status/2092477136774807888>; National Identification and Registration Authority, Uganda (15 May 2025). Press release on mass enrolment and renewal of national IDs. <https://www.nira.go.ug/publications/press-statement-on-the-mass-enrolment-exercise>; National Information Technology Authority–Uganda. (2026). Strategic plan FY2025/26–FY2029/30. <https://www.nita.go.ug/strategic-plans>
- 42 Uganda Communications Commission. (2026, January 14). Temporary suspension of public internet access and selected mobile services. <https://www.ucc.co.ug/wp-content/uploads/2026/01/Temporary-suspension-of-public-internet-access-and-mobile-services.pdf>; Uganda Communications Commission. (2026, January 18). Public update: Restoration of public internet access. <https://www.ucc.co.ug/public-update-18th-january-2026-press-briefing-to-update-the-country/>; High Court of Uganda, Civil Division. (2025, June 10). Initiative for Social and Economic Rights (ISER) and 2 others v. Attorney General and another (Miscellaneous Cause No. 0086 of 2022) [2025] UGHCCD 90. <https://ulii.org/en/akn/ug/judgement/ughccd/2025/90/eng@2025-06-10>
- 43 Supreme Court of Ghana. (2026, February 25). *Gorni v. Vodafone Ghana Ltd and others* (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>; Ghana Interbank Payment and Settlement Systems. (2026). Industry performance: 2025 transaction volume
- 44 Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry–NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>
- 45 State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026-into-law-as-minister-reveals-the-arrest-of-terrorists-with-nimc-database/>; Nigeria Inter-Bank Settlement System. (2025, June 23). NIBSS unveils the National Payment Stack to power the future of instant payments in Nigeria. <https://nibss-plc.com.ng/nibss-unveils-the-national-payment-stack-to-power-the-future-of-instant-payments->
- 46 Présidence du Sénégal. (2025, February 24). Launch of Senegal's new digital strategy 'New Deal Technologique'. <https://www.presidence.sn/en/actualites/launch-of-senegals-new-digital-strategy-newdeal-technologique-1/>
- 47 Ministry of Communication, Telecommunications and the Digital Economy, Senegal / Jokkoo. (2026, January 16). Inter-ministerial and interoperable
- 48 Community Court of Justice, ECOWAS. (2025, May 14). *L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal* (Application No. ECW/CCJ/APP/37/23; judgement No. ECW/CCJ/JUD/29/25). <https://africanlii.org/en/akn/aa/judgement/ecowas->
- 49 MyMzansi / Government of South Africa. (n.d.). Digital transformation roadmap. Retrieved September 13, 2026, from <https://www.mymzansi.gov.za/roadmap>; Government of South Africa / MyMzansi. (2025, May). Roadmap for the digital transformation of government. https://www.mymzansi.gov.za/static/resources/MyMzansi_Roadmap_Final_2025.pdf; Information Regulator of South Africa. (2026). Annual performance plan 2026/27. <https://info regulator.org.za/wp-content/>
- 50 World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>
- 51 Access Now / #KeepItOn. (2026). 2026 elections and internet shutdowns watch. <https://www.accessnow.org/campaign/2026-elections-and-internet-shutdowns-watch/>
- 52 National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>

Platform (Project Pangolin), making governance of future interoperability a present issue.⁵³ These cases show why current operational impact and foreseeable risks from funded or announced systems need to be assessed separately.

Across the 11 countries, there is no single regional sequence from digitisation to rights-respecting DPI. The common movement is toward deeper reuse of identity, payments and public data. The pace of legal reform, regulator independence, civic participation and remedy differs by country and as demonstrated across the countries, can change sharply within a year.

3.3 Continental Norms and Regional Instruments

The trend of continental digital-governance norms became more specific during 2024–2026, although legal uptake and enforcement remain uneven across countries. The AU Assembly adopted the Digital Transformation Strategy for Africa (2020–2030) in October 2019;⁵⁴ the AU Data Policy Framework in February 2022;⁵⁵ AfCFTA Protocol on Digital Trade on 18 February 2024;⁵⁶ the AU Executive Council endorsed the Continental Artificial Intelligence Strategy⁵⁷ and adopted the African Digital Compact⁵⁸ on 18–19 July 2024. The Executive Council also published data-provision guidelines for digital trade on 22 May 2025.⁵⁹ These instruments strengthen the policy basis for interoperable, inclusive and rights-aware digital systems, but none substitutes for domestic enforcement.

The continental democratic framework also became more explicit in 2026. Building on Resolution 580 of 8 March 2024, which condemned election-related internet shutdowns,⁶⁰ the African Commission on Human and Peoples' Rights (ACHPR) adopted Resolution 655 on Elections in Africa on 13 March 2026. The resolution called for independent electoral bodies, redress for election-related violations, an end to telecommunications and internet disruptions around elections, and stronger legal and monitoring responses to disinformation and emerging threats including artificial intelligence.⁶¹ International IDEA's January 2026 Democracy Stack paper similarly argues that DPI should be assessed against rights, rule of law, representation and participation, not only efficiency or service delivery.⁶²

The Malabo Convention, however, shows mixed results. Adopted on 27 June 2014, it only entered into force on 8 June 2023, nine years later, and even then, the AU status list dated 2 February 2026 recorded just 20 ratifications/deposits. Ghana, Senegal and Zambia are the ratifying parties among the study countries. Nigeria, South Africa and Tunisia are signatories that had not ratified, while Egypt, Ethiopia, Kenya, Uganda and Zimbabwe remained outside the treaty.⁶³ The evidence, therefore, indicates that within West, East, Southern and North Africa, national performance in the update and enforcement of continental instruments still varies substantially.

53 World Bank. (2021). Digital economy for Zimbabwe: Country diagnostic report. <https://documents1.worldbank.org/curated/en/982981621880260112/pdf/Digital-Economy-for-Zimbabwe-Country-Diagnostic-Report.pdf>; United Nations in Zimbabwe. (2026, March 14). Zimbabwe unveils 2026–2030 AI strategy to advance inclusive digital transformation. <https://zimbabwe.un.org/en/311859-zimbabwe-unveils-2026%E2%80%932030-ai-strategy-advance-inclusive-digital-transformation>

61. Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. https://zimbtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE_2026-National-Budget_25_November_2025-final.pdf

54 African Union. (2019, October), Digital Transformation Strategy for Africa (2020–2030) <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf>

55 African Union. (2022, February), Data Policy Framework <https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf>

56 African Union. (2024, February 18). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. https://opendata.pap.au.int/akn/aa-au/act/protocol/2024/free_trade_area_on_digital_trade/eng@2024-02-18/source.pdf

57 African Union. (2024, August 9). Continental Artificial Intelligence Strategy. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>

58 African Union. (2024, August 9). African Digital Compact. <https://au.int/en/node/44005>

59 African Union. (2025, May 22). Guidelines for integrating data provisions in protocols on digital trade. <https://au.int/en/documents/20250522/guidelines-integrating-data-provisions-protocols-digital-trade>

60 African Commission on Human and Peoples' Rights. (2024, March 8). Resolution on internet shutdowns and elections in Africa (ACHPR/Res.580 (LXXVIII) 2024). <https://achpr.au.int/en/adopted-resolutions/580-internet-shutdowns-elections-africa-achpres580-lxxviii>

61 African Commission on Human and Peoples' Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achpres655lxxvii-2026>

62 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/publications/catalogue/html/case-democracy-stack-rethinking-digital-public-infrastructure>

63 African Union. (2026, February 2). Status list: African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf

4.0 Research Findings

4.1 Overview of DPI in the Study Countries

Across the 11 study countries, DPI systems are at different stages of development but are increasingly performing similar functions as reusable infrastructure for public and private transactions. Countries are moving towards more interconnected digital identity, payment, data-exchange, and service systems, although they differ markedly in scale, sequencing, and institutional control.

Digital identity is relatively mature in many of the study countries and is increasingly serving as a reusable administrative key rather than a stand-alone credential. This can improve convenience and access to services, but it also increases the consequences of inaccurate, inaccessible or unavailable identity records.

Digital payments are also mature in several countries, while data-exchange systems are the least transparent and most unevenly developed layer. Importantly, technical maturity does not necessarily correspond with strong rights safeguards or effective oversight. The analysis therefore considers the technical development of DPI separately from the quality of rights-respecting governance surrounding it.

Table 2: Overview of DPI Systems

Country	Digital ID	Data Exchange	Digital Payments	Main e-government Portals	Key Institutions
Egypt	14-digit National Number; Haweya Biometric Digital Financial Identity (DFI) platform 37 banks on electronic Know Your Customer (eKYC)	<i>Digital Egypt</i> platform & Government Service Bus 33,000 linked institutions	<i>Meeza</i> domestic card scheme; <i>InstaPay</i> / Instant Payment Network (IPN) 43.5M <i>Meeza</i> cards; 55.5M wallets; 16.5M <i>Instapay</i> users	<i>Digital Egypt</i> , 12M registered users; 240+ services across 9 ministries	Civil Status Dept, Ministry of Interior, Central Bank of Egypt (CBE), Egyptian Banks Company (EBC), Ministry of Communications & IT (MCIT)
Ethiopia	<i>Fayda</i> (MOSIP-based 12-digit foundational biometric ID) 50M registered	<i>EthioConnect</i> Interoperability Layer	<i>Telebirr</i> Mobile Money Rail, <i>EthSwitch</i> , & Commercial Bank of Ethiopia (CBE) Digital Banking 54M registered users	<i>MESOB</i> (Modern Ethiopia Service for Organized Benefits) Portal 185 integrated public services	National ID Program; <i>Faydaverse</i> (under Ethiopian Investment Holdings / PM Office); <i>Ethio Telecom</i> ; National Bank of Ethiopia (NBE); Ethiopian AI Institute; Federal Civil Service Commission
Ghana	<i>Ghana Card</i> (Integrated Identity System) 20.1M enrolled	National Data Exchange Platform & e-GIF Framework v2.0	<i>GhIPSS</i> , <i>GhIPSS</i> Instant Pay (GIP), Mobile Money Interoperability (MMI), <i>e-Zwich</i> 26M active mobile wallets; 2.89M <i>e-Zwich</i> cards	<i>CitizenApp</i> & <i>Ghana.gov</i> Portal	National Identification Authority (NIA); <i>GhIPSS</i> ; Bank of Ghana; National Information Technology Agency (NITA); Ministry of Communication, Digital Technology & Innovations

Kenya	Maisha Namba Ecosystem (I, (3rd-Gen Maisha Card), Maisha Digital ID, Master Population Register	GavaConnect API Framework & SHA Health Information Exchange	M-Pesa & Mobile Money; Treasury Payment Integrations; PAPSS; Pesalink 53M mobile money accounts	<i>eCitizen Portal</i> 28,373 onboarded public services; 5,731 operational. 30+ other fragmented portals	State Dept for Immigration & Citizen Services; National Registration Bureau (NRB); Ministry of Information, Communications and the Digital Economy (MICDE); Safaricom, Central Bank of Kenya (CBK); Kenya Bankers Association; ICT Authority; Social Health Authority (SHA); Webmasters Kenya Limited; Pesaflo Limited, and Olive Tree Media Limited
Nigeria	National Identification Number (NIN) & National Identity Database (NIDB) 136M enrolled	Nigerian Data Exchange (NGDX) & NIMC Verification APIs / Life Events Framework	Bank Verification Number (BVN), NIBSS Instant Payment (NIP), & National Payment Stack 136 NINs linked	e-Tax, Treasury Single Account (TSA), & Social Investment Register	National Identity Management Commission (NIMC); Nigeria Inter-Bank Settlement System Plc (NIBSS); Central Bank of Nigeria (CBN); National Information Technology Development Agency (NITDA); Federal Ministry of Communications, Innovation & Digital Economy
Senegal	ECOWAS Biometric Identity Card (CE-DEAO / eID) & National Civil Registry (RNEC) 20M civil status records digitised; 10M+ enrolled	Jokkoo / PINS (GovStack inter-ministerial data exchange layer based on X-Road)	Wave, Orange Money, Free Money, & BCEAO PI-SPI Regional Instant Rail	<i>e-Senegal</i> / Senegal Services Platform & <i>e-DGID</i> (Tax) 800–900 administrative procedures	National Civil Status Agency (ANEC); Direction AI (DAF); Ministry of Interior; Central Bank of West African States (BCEAO); private operators (Sonatel, Wave); SENUM S.A.; Ministry of Communication & Telecoms; Directorate General of Taxes and Property (DGID)
South Africa	Smart ID Card & MyMzansi Digital Identity Credential Issued through 200+ bank branches	MzansiXchange Layer pilot modelled on X-Road targeting 20+ government registries	PayShap (with ShapID alias) & Real-Time Clearance (RTC)	MyMzansi Portal & Revamped Gov.za	National Treasury & Presidency Digital Services Unit (DSU); Department of Home Affairs (DHA); South African Reserve Bank (SARB), PASA & BankserveAfrica; DCDT
Tunisia	Unique Citizen Identifier (IUC), <i>e-Houwiya</i> (Mobile ID), & Biometric CIN 200,000 <i>e-Houwiya</i> subscribers	TunXRoad / RNIA2 Data Exchange Layer Shared exchange layer linking MADANIA civil status, tax, property, and vehicle registries	Central Bank Remote Onboarding / eKYC Digital Payment Rails Integrated with <i>e-Houwiya</i>	<i>E-Bawaba</i> National Portal & <i>E-CNAM</i> (Social Security) Single sign-on public services authenticated via <i>e-Houwiya</i> Mobile ID	Ministry of Communication Technologies (<i>e-Houwiya</i>); Ministry of Interior (CIN); Central Bank of Tunisia (BCT); Centre National de l'Informatique (CNI); Ministry of Communication Technologies; Ministry of Communication Technologies & CNAM
Uganda	Ndaga Muntu (National ID migrated to open-source MOSIP in 2025) 35M+ enrolled	Integration Services Platform (UGHub) Connected 135 entities (62 public, 73 private); covers 37% of MDAs	Mobile Money (MTN, Airtel), UNISS, ACH, & Bank of Uganda Payment Switch 36.3M active mobile money accounts	<i>EFRIS</i> (Tax), Express Penalty Scheme, ECCMIS (Judiciary), & e-GP	National Identification and Registration Authority (NIRA); Bank of Uganda (BoU) & telecom operators (MTN, Airtel); National Information Technology Authority Uganda (NITA-U); Uganda Revenue Authority (URA), & Ministry of ICT

Zambia	Integrated National Registration Information System (INRIS / MOSIP ID) & National Registration Card (NRC) 1.5M enrolled on INRIS	Government Service Bus (GSB) / ZamConnect Exchange Platform	National Financial Switch (NFS) & ZamPay Gateway	<i>ZamPortal</i> (E-Services Portal) & ZamPass (Single Sign-On Portal)	Department of National Registration, Passport & Citizenship (DNRPC, Home Affairs); Bank of Zambia (BoZ); ZECHL; SMART Zambia Institute (SZI / Office of the President) & the Zambia Information and Communications Technology Authority (ZICTA)
Zimbabwe	Biometric National ID & Zimbabwe Population Registry System (ZPRS)	<i>ZimConnect</i> Service Platform, National Data Centre, & <i>Project Pangolin</i>	<i>Zimswitch</i> National Switch & ZIMSWITCH Instant Payment Interchange Technology (ZIPIT) Instant Rail (<i>EcoCash</i> , <i>OneMoney</i>)	<i>ZimPortal</i> / Government Portal, ASYCUDA World (Customs), & electronic Government Procurement (eGP) system	Civil Registry Department (Ministry of Home Affairs & Cultural Heritage); Reserve Bank of Zimbabwe (RBZ) & Zimswitch Technologies Pvt Ltd; Ministry of ICT, Postal & Courier Services; Government ISP (GISP); Ministry of ICT; Zimbabwe Revenue Authority (ZIMRA) Procurement Regulatory Authority (PRAZ)

Egypt continues to layer digital government and financial identity services onto its National Number system.⁶⁴ Tunisia combines a longstanding civil-registration base, the Unique Citizen Identifier and Mobile ID; the 1 July 2026 investment rule shows how voluntary digital identity can become mandatory one sector at a time.⁶⁵

In East Africa, Ethiopia, Kenya, and Uganda illustrate different forms of integration. Ethiopia's Fayda, MESOB, Telebirr, and developing data-exchange functions are being built as mutually reinforcing layers, and Faydaverse now has a state-owned commercial and operational mandate to scale the infrastructure.⁶⁶ Kenya's National ID and Maisha Namba Digital ID are being introduced into an already mature eCitizen and mobile-money environment supporting various services.⁶⁷ Uganda's NIRA and UGHub are already sufficiently central to government and private services that an error in a foundational record can affect several downstream interactions.⁶⁸ The progressive potential is reduced duplication and easier authentication. The corresponding risk is that errors in a public record, and the exclusion they cause, can also become entrenched.

West Africa has some of the most mature payment examples. Ghana's Ghana Card is widely used for verification, while GhIPSS and Mobile Money Interoperability provide high-volume payment rails.⁶⁹ Nigeria combines the NIN, Bank Verification Number, and NIBSS infrastructure at a very large scale, and NIBSS launched the National Payment Stack on 23 June 2025.⁷⁰ Senegal's iden-

⁶⁴ State Information Service, Egypt. (2026, July 21). Communications Minister: Egypt to offer more than 270 digital government services by end-2026. <https://sis.gov.eg/en/media-center/news/communications-minister-egypt-to-offer-more-than-270-digital-government-services-by-end-2026/>; Central Bank of Egypt. (2025, November 16). PAFIX 2025: Digital Financial Identity platform (Haweya). <https://www.cbe.org.eg/en/news-publications/news/2025/11/16/18/47/pafix-2025>

⁶⁵ Ministry of Communication Technologies, Tunisia. (n.d.). e-Houwiya / Mobile ID. Retrieved September 13, 2026, from <https://www.mobile-id.tn/accueil>; Tunis Afrique Presse / Tunisian Investment Authority. (2026, June 24). "Mobile ID" mandatory for project declarations from 1 July 2026. <https://www.tap.info.tn/en/Portal-Economy/20326511--mobile-id>; Tunisia Legal Database / DCAF. (2020, May 12). Decree-Law No. 2020-17 on the Unique Citizen Identifier. <https://legislation-securite.tn/latest-laws/decret-loi-du-chef-du-gouvernement-n-2020-17-du-12-mai-2020-relatif-a-l'identifiant-unique-du-citoyen/>

⁶⁶ Fayda National ID, Ethiopia (accessed 13 September 2026). Official programme overview — foundational digital ID under Proclamation No. 1284/2023. <https://www.id.gov.et/>; Ethiopian Investment Holdings. (2026, August 4). National ID Program reestablished as state-owned enterprise "Faydaverse" to anchor nationwide digital public infrastructure. <https://eih.et/national-id-program-reestablished-as-state-owned-enterprise-faydaverse-to-anchor-nationwide-digital-public-infrastructure-and-joins-ethiopian-investment-holdings-portfolio/>; Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethiotelcom.et/2025-26-budget-year-annual-business-performance-report/5/>

⁶⁷ Directorate of Immigration Services, Kenya. (2024, September 19). Issuance of Maisha Card IDs. <https://immigration.go.ke/issuance-of-maisha-card-ids/>; eCitizen (n.d.). What Digital ID offers <https://did.ecitizen.go.ke/>

⁶⁸ National Information Technology Authority–Uganda (NITA-U) on X, <https://x.com/NITAUGanda1/status/2092477136774807888>; National Identification and Registration Authority, Uganda. (2025, May 15). Press statement on the mass enrolment exercise. <https://www.nira.go.ug/publications/press-statement-on-the-mass-enrolment-exercise>

⁶⁹ National Identification Authority, Ghana. (n.d.). Home. Retrieved September 13, 2026, from <https://nia.gov.gh/>; Ghana Interbank Payment and Settlement Systems. (2026). Industry performance: 2025 transaction volume and value. <https://ghipss.net/component/content/category/56-newsletters>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory-for-ghana-card-verification-under-new-l-i-2523/>

⁷⁰ Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry–NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>; Nigeria Inter-Bank Settlement System. (2025, June 23). NIBSS unveils the National Payment Stack to power the future of instant payments in Nigeria. <https://nibss-plc.com.ng/nibss-unveils-the-national-payment-stack-to-power-the-future-of-instant-payments-in-nigeria/>

tity and civil-status systems are more institutionally distributed, but the government's 2025 New Deal Technologique and the inter-ministerial data-exchange project described in January 2026 point toward a more connected state architecture.⁷¹

In Southern Africa, South Africa is deliberately phasing in the newer DPI stack. Whereas the Smart ID and National Population Register are well established, MzansiXchange is being piloted as a federated exchange layer, and the functional Digital ID is intended to coexist with physical credentials.⁷² Zambia is moving toward new digital identity and interoperable government services under the Digital Zambia Acceleration Project; its existing National Financial Switch already provides shared retail-payment infrastructure.⁷³ Zimbabwe has a population registry system and instant payment technologies but has not consolidated identity, payments, and public data into a single national stack. However, its 2026–2030 AI strategy and Project Pangolin would create a more significant national data layer if implemented as planned.⁷⁴ The Southern African cases therefore include both phased integration and systems whose main rights effects are still prospective.

Across the study countries, no single country leads on all dimensions of DPI (maturity; scale, frequency of use, interoperability, or institutional completeness). Nigeria and Ethiopia lead in identity expansion, Ghana, Kenya, and South Africa have more developed payment and service ecosystems, while Uganda highlights risks of mandatory linkages. Others, including Tunisia, Senegal, Zambia, and Zimbabwe, remain at nascent stages where current choices will shape future outcomes. Overall, DPI maturity is uneven, constrained by gaps in data-sharing infrastructure, incomplete enrolment, and weak governance frameworks.

Additionally, DPI depends on international fibre cables, satellite, fixed and mobile networks, local internet exchange points, data centres and cloud hosting, devices, service points and electricity. Connectivity has increasingly become a pre-condition for both access to essential services and democratic participation. As DPI systems become more connected, a cable cut, power failure, cloud outage or internet disruption can simultaneously interrupt identity, payments and public services, affecting both socio-economic and civil and political rights. On 14 March 2024, the failure of four submarine cables (affecting the WACS, MainOne, SAT-3 and ACE systems) off Cote d'Ivoire affected 13 African countries and showed that separate cables can share one physical point of failure.⁷⁵ Diverse routes, cross-border fibre, operational internet exchange points and local content helped maintain connectivity. For landlocked Ethiopia, Uganda, Zambia and Zimbabwe, resilience also depends on neighbouring states, border crossings and regional restoration arrangements.

On June 25, 2024, a seven-hour total internet disruption in Kenya during the youth-led #RejectFinanceBill2024 protests affected connectivity and cloud services in neighbouring Burundi, Rwanda and Uganda, highlighting these countries' dependence on Kenyan transit routes for their International connectivity.⁷⁶ Further, infrastructure coverage is supplemented by meaningful use, which includes affordability, device access, speed, reliability, skills, disability access, successful service completion and continuity.⁷⁷ As data processing becomes more mainstream, Africa's 72 data centres remain concentrated in Egypt, Kenya, Nigeria and South Africa.⁷⁸ Investment in such data centres will also place new demands on electricity, water, and land, while also impacting labour and climate.⁷⁹

71 Présidence du Sénégal. (2025, February 24). Launch of Senegal's new digital strategy 'New Deal Technologique'. <https://www.presidence.sn/en/actualites/launch-of-senegals-new-digital-strategy-newdeal-technologique-1/>; Ministry of Communication, Telecommunications and the Digital Economy, Senegal / Jikkoo. (2026). National interoperability platform (PINS/Jikkoo). <https://www.pins.sn/>; Ministry of Communication, Telecommunications and the Digital Economy, Senegal / Jikkoo. (2026, January 16). Inter-ministerial and interoperable data-exchange platform of Senegal. <https://pins.sn/actualites/2026-01/plateforme-interministerielle-et-interoperable-dechange-de-donnees-du-senegal>

72 MyMzansi / Government of South Africa. (n.d.). Digital transformation roadmap. Retrieved September 13, 2026, from <https://www.mymzansi.gov.za/roadmap>; Government of South Africa / MyMzansi. (2025, May). Roadmap for the digital transformation of government. https://www.mymzansi.gov.za/static/resources/MyMzansi_Roadmap_Final_2025.pdf; SAnews. (2026, June 24). More than 200 bank branches now offering Smart ID card. <https://www.sanews.gov.za/south-africa/more-200-bank-branches-now-offering-smart-id-card>

73 World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>; Bank of Zambia. (2023). National Payment Systems Annual Report 2022. https://www.boz.zm/2022NationalPaymentsSystemsAnnualReport_FINAL.pdf

74 World Bank. (2021). Digital economy for Zimbabwe: Country diagnostic report. <https://documents1.worldbank.org/curated/en/982981621880260112/pdf/Digital-Economy-for-Zimbabwe-Country-Diagnostic-Report.pdf>; United Nations in Zimbabwe. (2026, March 14). Zimbabwe unveils 2026–2030 AI strategy to advance inclusive digital transformation. <https://zimbabwe.un.org/en/311859-zimbabwe-unveils-2026%E2%80%932030-ai-strategy-advance-inclusive-digital-transformation>; Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. https://zimtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE_2026-National-Budget_25_November_2025-final.pdf

75 Internet Society, 2024 West Africa Submarine Cable Outage Report <https://www.internetsociety.org/resources/doc/2024/2024-west-africa-submarine-cable-outage-report/>

76 KICTANet. (2024, June 26). Kenya's Internet Disrupted During Protests: A Violation of Human Rights <https://www.kictanet.or.ke/kenyas-internet-disrupted-during-protests-a-violation-of-human-rights/>

77 World Bank, Digital Progress and Trends Report 2023 <https://www.worldbank.org/en/publication/digital-progress-and-trends-report>; ^[1] International Telecommunication Union, Facts and Figures 2024 <https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/>

78 Teraco (Digital Realty), 'Africa's data centres and cloud infrastructure: growth, connectivity, and digital transformation' — summarising the 2026 Africa Interconnection Report (Balancing Act) — <https://www.teraco.co.za/blog/africas-data-centres-and-cloud-infrastructure-growth-connectivity-and-digital-transformation/>

79 International Energy Agency, Data Centres and Data Transmission Networks <https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks>

4.1.1 Digital Identity and Data Exchange Systems

Digital Public Infrastructure systems do not conform to a single, uniform technical architecture. Instead, national digital ID systems demonstrate four distinct entry ecosystems – identification-led, payment-led, authentication-led, and plural national-led. These pathways are shaped by legacy administrative structures, institutional design, degree of centralisation, market maturity, and governance safeguards.⁸⁰

The first are identification-led ecosystems such as those found in Egypt, Senegal, South Africa, Tunisia, Uganda, Zambia and Zimbabwe whose dominant foundational civil registries, national identity cards, or population registers evolved first or independently before connecting to data-exchange or payment layers for digital authentication. Uganda provides a recent example of this expanding reuse of foundational identity. In early September, the Cabinet approved the use of the National Identification Number (NIN) as the Tax Identification Number (TIN) for individual taxpayers in what has been described as “the government’s broader effort to integrate public databases, improve the accuracy of taxpayer information and strengthen domestic revenue mobilisation.”⁸¹ South Africa operates a transitional model under its MyMzansi Roadmap, where an optional Digital ID credential coexists with physical Smart ID cards, linked to the MzansiXchange data layer and PayShap instant payment switch.⁸²

Tunisia’s legacy civil registers (MADANIA) are linked to the TunXRoad/RNIA2 federated exchange layer using UXP security adapters, the Unique Citizen Identifier (IUC), and Mobile ID (e-Houwiya), while rolling out mandatory biometric national ID cards (CIN) under Organic Law No. 2024-22.⁸³ Egypt’s 14-digit National Number issued by the Interior Ministry is linked to Digital Egypt across 33,000 institutions via the Government Service Bus, retail payment rails (Meeza cards and InstaPay and the Central Bank-approved Haweya Digital Financial Identity (DFI/eKYC) platform serving 37 banks.⁸⁴ Zimbabwe is now rolling out biometric identity cards, and payments run through EcoCash, Zimswitch and ZIPIT national payment rails while data exchange is planned through ZimConnect and the Project Pangolin data platform.⁸⁵

The second are payment-led ecosystems such as Kenya’s Maisha Namba and Nigeria’s NIN, which have at least one identification scheme that is digitally authenticated and whose initial primary adoption was influenced by its linkage with the national payments system such as mobile money, commercial banking and retail instant switches. In Kenya, M-Pesa, which has at least 53 million accounts, serves as the primary payment system, and registered SIM cards are an authentication layer for the eCitizen portal, now governed under the Public Finance Management (E-Citizen System Management) Regulations, 2026.⁸⁶

Kenya’s GavaConnect, launched in November 2024, provides an official API environment through which approved users can integrate government data and services.⁸⁷ Further, in the health sector, the Digital Health Act, 2023 (No. 15 of 2023), established the Digital Health Agency and a comprehensive integrated health information system.⁸⁸ The Digital Health (Data Exchange Component) Regulations, 2025 (Legal Notice No. 77 of 2025), adds rules on secure data exchange, purpose limitation, access controls, audit logs, and interoperability.⁸⁹ These developments place Kenya among the countries moving from portal-based digitisation-

⁸⁰ Klaaren, J. (2026). Digital public infrastructure across Africa: A national identity systems perspective. African Journal of Information and Communication, 37. <https://ajic.wits.ac.za/article/view/25654/26029>

⁸¹ Daily Monitor. (2026, September 8). Why your NIN is replacing your TIN <https://www.monitor.co.ug/uganda/business/prosper/why-your-nin-is-replacing-your-tin-5586362>

⁸² National Treasury. (2025). MzansiXchange: About. <https://mzansixchange.treasury.gov.za/about/>; National Treasury. (2025, October 9). MzansiXchange pilot launch address. <https://www.gov.za/news/speeches/director-general-duncan-pieterse-mzansixchange-pilot-launch-09-oct-2025>

⁸³ ID Tech (MobileIDWorld syndication). (2025). *E-Houwiya: A Milestone in Tunisia’s Digital Transformation Roadmap 2025 <https://idtechwire.com/e-houwiya-a-milestone-in-tunisias-digital-transformation-roadmap-2025/>

⁸⁴ E-Government Development in Egypt <https://we.hse.ru/en/irs/cas/passeq>; Egypt launches digital licensing service for public establishments through Egypt Digital Platform <https://techreviewafrica.com/news/6482/egypt-launches-digital-licensing-service-for-public-establishments-through-egypt-digital-platform>; The Central Bank of Egypt Issues Regulations Governing the Services of the Digital Financial Identity Platform for Identifying Bank Customers and Verifying their Identities Electronically (eKYC) <https://www.cbe.org.eg/en/news-publications/news/2026/08/24/09/40/ekyc-2026>; Egypt approves banking sector eKYC legal framework in financial inclusion push <https://www.biometricupdate.com/202608/egypt-approves-banking-sector-ekyc-legal-framework-in-financial-inclusion-push>

⁸⁵ AGCNewsNet, ‘Zimbabwean Government Announces Move to Roll Out Digital IDs’, May 2024 <https://www.agcnewsnet.com/article/4753>; AfricaNenda, ‘SIIPS 2024: ZIPIT Case Study (Zimbabwe)’. https://www.africanenda.org/uploads/files/siips_2024_ZIPIT_CaseStudy_en.pdf; Reserve Bank of Zimbabwe, Press Statement: ‘Designation of Zimswitch Technologies as National Payment Switch’, 9 July 2020. https://www.rbz.co.zw/documents/press/July/00100_Press-Statement---Zimswitch-Designation-as-National-Switch---9-7-2020-2.pdf

⁸⁶ Republic of Kenya (2026). The Public Finance Management (E-Citizen System Management) Regulations, 2026 <https://kenyalaw.org/akn/ke/act/In/2026/135/eng@2026-07-23>

⁸⁷ MyGov, Kenya. (2024, November 13). KRA launches ‘GavaConnect’ API to modernize tax administration and spur innovation. <https://gaa.go.ke/kra-launches-gava-connect-api-modernize-tax-administration-and-spur-innovation>; Kenya Revenue Authority. (n.d.). GavaConnect developer portal. Retrieved September 11, 2026, from <https://developer.go.ke/>

⁸⁸ Kenya Law. (2023). Digital Health Act, 2023 (No. 15 of 2023). <https://new.kenyalaw.org/akn/ke/act/2023/15/eng@2023-11-24>

⁸⁹ Kenya Law. (2025, April 11). Digital Health (Data Exchange Component) Regulations, 2025 (Legal Notice No. 77 of 2025). <https://new.kenyalaw.org/akn/ke/act/In/2025/77/eng@2025-04-11/source>

toward reusable data exchange infrastructure, while also demonstrating that sector-specific safeguards can be more developed than whole-of-government API governance.

Third, are the authentication-led ecosystems such as Ethiopia's MOSIP-based *Fayda* Digital ID, which has a dominant centralised biometric digital foundational identity built from the outset as an authentication gateway for banking, tax and government services. *Fayda* is required for all bank account openings, tax registration, and logins to *MESOB*, the unified e-government super-app offering over 185 public services.⁹⁰ Ethiopia's institutional model also changed on 4 August 2026 when Ethiopian Investment Holdings re-established the National ID Programme as the state-owned *Faydaverse*, mandated to operate and scale national DPI.⁹¹ The implication from a rights perspective is that the quality and correction of one record increasingly matters across several domains.

The fourth is a plural national identity system such as the Ghana Card, which has multiple identification schemes, at least one of which is digitally authenticated but without any being dominant, and is linked to as an equal to the national payments system and data exchange.

The reuse of identity is equally expanding beyond ordinary service delivery. In Ghana, Egypt, Kenya, Nigeria, Senegal, Uganda, Zambia and Zimbabwe, the reuse of digital identity systems for electoral purposes extends to electoral eligibility, verification and voter register maintenance. Another element is the role of mandatory SIM card registration as a secondary identity layer connecting foundational identity to telecommunications and financial services. Making digital ID mandatory for SIM activation, elections, and banking converts technical glitches, biometric read failures, or administrative delays into immediate, cascading exclusion from economic and social life, whose effect has been seen in Ghana, Nigeria, and Uganda. Design choice is not simply whether systems interoperate, but whether they exchange the minimum attributes necessary under auditable rules or create broad, persistent access to foundational records. The AU Interoperability Framework for Digital ID supports minimisation and trust-based interoperability rather than unrestricted data pooling.⁹²

4.1.2 Narratives Justifying DPI Deployment

Justifications for DPI rollout can be classified along two broad narratives. The first are the countries that prioritise inclusion, digital transformation and the modernisation of government administration. This narrative is promoted by state communications, central banks, and development partners e.g., World Bank ID4D, MOSIP (Gates Foundation, 50-in5 Campaign, among others) evident in Nigeria and Ethiopia.⁹³ It frames DPI as a public interest necessity needed to expand financial inclusion, streamline service delivery, eliminate fraud, and formalise the informal economy. Ethiopia presents *Fayda* as an inclusion and service-delivery platform and has linked it to a broader data-sovereignty agenda.⁹⁴ Nigeria's NIMC Act, 2026 expressly links identity management to public service delivery, economic transformation, database harmonisation and national security.⁹⁵ Senegal's New Deal Technologique and South Africa's MyMzansi roadmap emphasise sovereignty and whole-of-government modernisation.⁹⁶ In Egypt,

90 Biometric Update (2025). Mandatory digital ID for banking policy goes into effect in Ethiopia. 6 Jan 2025. <https://www.biometricupdate.com/202501/mandatory-digital-id-for-banking-policy-goes-into-effect-in-ethiopia>

91 Ethiopian Investment Holdings. (2026, August 4). National ID Program reestablished as state-owned enterprise "Faydaverse" to anchor nationwide digital public infrastructure. <https://eih.et/national-id-program-reestablished-as-state-owned-enterprise-faydaverse-to-anchor-nationwide-digital-public-infrastructure>

92 African Union Commission. (2023, December 11). AU interoperability framework for digital ID. https://www.au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf

93 Integrated Biometrics (2026). *Ethiopia: Fayda ID and Integrated Biometrics Bring Digital Inclusion*. Feb 2026. <https://integratedbiometrics.com/feature/ethiopia-fayda-id-and-integrated-biometrics-bring-digital-inclusion>; Biometric Update (2024). *World Bank extends Nigeria digital ID project support by another two years*. 31 Dec 2024 <https://www.biometricupdate.com/202412/world-bank-extends-nigeria-digital-id-project-support-by-another-two-years>; UNDP (2024). *11 'First-Mover' Countries Launch 50-in-5 Campaign to Accelerate Digital Public Infrastructure Adoption Around the World*. <https://www.undp.org/news/11-first-mover-countries-launch-50-5-campaign-accelerate-digital-public-infrastructure-adoption-around-world>; Biometric Update (2025). *Gates Foundation Fuels Senegal's Digital Transformation with \$10M*. 29 Sep 2025. Retrieved from <https://www.biometricupdate.com/202509/gates-foundation-fuels-senegals-digital-transformation>

94 *Fayda* National ID, Ethiopia (accessed 13 September 2026). Official programme overview — foundational digital ID under Proclamation No. 1284/2023. <https://www.id.gov.et/>; Ethiopian Investment Holdings. (2026, August 4). National ID Program reestablished as state-owned enterprise "Faydaverse" to anchor nationwide digital public infrastructure. <https://eih.et/national-id-program-reestablished-as-state-owned-enterprise-faydaverse-to-anchor-nationwide-digital-public-infrastructure-and-joins-ethiopian-investment-holdings-portfolio/>

95 State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026>

96 Présidence du Sénégal. (2025, February 24). Launch of Senegal's new digital strategy 'New Deal Technologique'. <https://www.presidence.sn/en/actualites/launch-of-senegals-new-digital-strategy-newdeal-technologique-1/>; MyMzansi / Government of South Africa. (n.d.). Digital transformation roadmap. Retrieved September 13, 2026, from <https://www.mymzansi.gov.za/roadmap>

the drive for a biometric digital ID is part of the country's digital transformation under Vision 2030 and Egypt ICT 2030 Strategy.⁹⁷

Ghana's DPI is framed as a continental success model for revenue mobilisation and financial inclusion.⁹⁸ The Ghana Revenue Authority (GRA) and National Health Insurance Scheme (NHIS) require Ghana Card verification for tax filing and healthcare.⁹⁹ Kenya provides a current example of this narrative broadening. At a DPI Roadmap development meeting on 12 September 2025, the MICDE described digital identity, secure payments, trusted data exchange and digital platforms as foundations for service delivery, innovation and competitiveness, while identifying inclusivity, trust and security, interoperability, innovation and sustainability as guiding pillars.¹⁰⁰ By February 2026, the same Ministry was framing data governance in terms of public trust, data rights and human-centric governance as well as economic value.¹⁰¹ This is a progressive shift in official language, although implementation remains the test.

The second narrative is on state control, surveillance, and national security. It operates alongside the inclusion goals and is used by state security, intelligence, and tax authorities to enforce compliance, monitor populations, fight corruption, expand tax collection, and enhance state legibility. In Uganda, the national ID system was originally conceived as the National Security Information System (NSIS), explicitly designed to identify, locate, and monitor citizens as part of broader national security functions.¹⁰² The Registration of Persons Act links national identification directly to voter administration.¹⁰³ In Egypt, the 14-digit National Number, digital service portals, and smart city technologies with facial recognition have expanded state tracking of citizens in an environment lacking an independent DPA.¹⁰⁴ The state has refused to renew ID documents of dissidents, journalists, and human rights activists living abroad. In Tunisia, the transition to biometric CIN cards under Law 2024-22 rests almost exclusively on security claims, backed by Decree-Law 54 used to prosecute online dissent and concerns over privacy given the outdated legal framework and civil society exclusion from the development process.¹⁰⁵ Zambia combines service modernisation with a more security-centred cyber-law framework.¹⁰⁶ There is a clearer public-purpose case, but the continuing challenge is to test stated purposes against actual outcomes and secondary uses.

Across Africa, electoral integrity, national security and data sovereignty are increasingly joining service efficiency as reasons for linking identity and data systems.¹⁰⁷ While these purposes may be legitimate, they have different rights implications and should not be collapsed into a single modernisation narrative. Election use, in particular, raises higher requirements for political neutrality, equal access and timely remedy because errors become constitutionally time-sensitive.¹⁰⁸

97 Abrougui, Afef; Farahat, Mohamed (2025). Digital-ID in Egypt: Country Report. The Institute of Development Studies and Partner Organisations. Chapter. <https://doi.org/10.19088/IDS.2025.057>

98 IdealToola Research. Ghana's Digital Payments Revolution: Interoperability, QR Codes & the Super-App Race. <https://ideatoola.com/data-stories/ghanas-digital-payments-revolution-interoperability-qr-codes-and-the-super-app-r>

99 National Identification Authority. Identity Verification Services. <https://nia.gov.gh/service/verification-services/>; Bank of Ghana, Use of Ghana Card for all Financial Transactions", (2022) <https://www.bog.gov.gh/notice/use-of-ghana-card-for-all-financial-transactions/>

100 Ministry of Information, Communications and the Digital Economy, Kenya. (2026, February 6). Government moves to strengthen Kenya's data governance framework. <https://ict.go.ke/government-moves-strengthen-kenyas-data-governance-framework>

101 Ministry of Information, Communications and the Digital Economy, Kenya. (2025, September 12). Government reaffirms its commitment to building an inclusive and trusted digital public infrastructure. <https://ict.go.ke/government-reaffirms-its-commitment-building-inclusive-and-trusted-digital-public-infrastructure>

102 Center for Human Rights and Global Justice (CHRGJ), Initiative for Social and Economic Rights (ISER) and Unwanted Witness, Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 2021. <https://iser-uganda.org/publication/chased-away-and-left-to-die/>

103 Uganda Legal Information Institute. (2015). Registration of Persons Act (Cap. 332), ss. 65–66. <https://ulii.org/en/akn/ug/act/2015/4/eng@2015-03-26>

104 Abrougui, Afef; Farahat, Mohamed (2025). Digital-ID in Egypt: Country Report. The Institute of Development Studies and Partner Organisations. Chapter. <https://doi.org/10.19088/IDS.2025.057>

105 Tunisia: IPI demands an end to repressive use of cybercrime law against journalists <https://ipi.media/tunisia-ipi-demands-an-end-to-repressive-use-of-cybercrime-law-against-journalists/>; Tunisia drives digitization agenda forward while navigating risks <https://www.biometricupdate.com/202503/tunisia-drives-digitization-agenda-forward-while-navigating-risks>; Tunisia's digitization programs threaten the privacy of millions <https://smex.org/tunisias-digitization-programs-threaten-the-privacy-of-millions/>

106 CIPESA. (2025, May 19). Zambia's cybersecurity and cybercrimes laws raise alarms for digital rights. <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/>; World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>; National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>

107 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>; International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

108 African Commission on Human and Peoples' Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achprres655lxxxvi-2026>

The information environment around DPI also affects democratic scrutiny. CIPESA's 2025 baseline study of media coverage in seven Eastern African countries found that Kenya recorded 199 DPI/DPG stories across the four sampled outlets in 2024, the second-highest volume after Tanzania.¹⁰⁹ Yet only 27.7% of Kenyan stories originated from independent reporting, with government actors (officialdom) accounting for 52.3% of newsmakers. The concern, therefore, is not that media coverage is absent, but that a predominantly official and event-driven framing can narrow public debate on privacy, exclusion, procurement and accountability unless independent reporting keeps pace with the expansion of DPI.

4.1.3 Objectives, Priorities and Interests Shaping DPI

African DPI financing, technical infrastructure and vendor choices influence the architecture, milestones and long-term dependency, but the evidence does not support treating all external involvement as a single model. The major external financiers underwriting major DPI rollouts are the World Bank (ID4D), Gates Foundation, Co-Develop, 50-in-5 Campaign, MOSIP, which target inclusion and prioritise mass digital ID enrollment, open standards, and payment interoperability. Ethiopia's official project page records US\$350 million in World Bank financing for Fayda, including a USD 50 million grant window for host communities and refugees.¹¹⁰

Nigeria has received a joint credit of USD 430 million from the World Bank (USD 115 million), French Development Agency (USD 100 million), and the European Investment Bank (USD 215 million).¹¹¹ In 2024, AFD and EIB threatened to cancel co-financing if the World Bank ceased as lead implementer, forcing a project extension to June 2026, to maintain continuity and safeguard the progress made. In Senegal, the World Bank and the Gates Foundation financing is supporting the New Deal Technologique and WURI Digital Identity Exchange.¹¹² In Tunisia, the World Bank is supporting GovTech digital transformation, while in Zambia it is supporting digital acceleration.¹¹³

Notably, multilateral funding is tied to aggressive, volume driven enrollment targets such as the World Bank requiring Nigeria NIN registrations to reach 180 million by December 2026, or the 90 million enrollment target for Fayda. When disbursement milestones reward speed and scale, national authorities are incentivised to deploy coercive approaches as was the case in Kenya's Huduma Namba, prior to establishing independent oversight, DPIA's or effective offline grievance channels.¹¹⁴

The state security and surveillance track is evidenced by investments in state security and public order technologies. In Egypt, US vendor Honeywell supplied a 6,000-camera surveillance network across the New Administrative Capital, operating alongside Huawei smart-city investments.¹¹⁵ At least 11 African countries, including Egypt, Kenya, Nigeria, Senegal, Uganda, Zambia and Zimbabwe, have invested over USD 2 billion in Chinese-supplied and AI-powered "smart city" and "safe city" surveillance infrastructure, used to monitor public spaces.¹¹⁶

Open-source identity platforms such as MOSIP can reduce some forms of vendor lock-in, while foreign commercial suppliers remain important elsewhere. Security and surveillance infrastructure follows different commercial and geopolitical channels. The key governance question is whether national institutions retain auditability, procurement transparency, technical exit options, and responsibility for rights impacts.

External involvement is not in itself evidence of a rights problem. The governance question is whether public institutions disclose who finances and supplies critical systems, what contractual and technical dependencies follow, which party is responsible for data protection and security, and what remedy is available when a private intermediary performs a public function. The UNGPs

109 CIPESA. (2025, October). Media coverage of digital public infrastructure and digital public goods in Eastern Africa. <https://cipesa.org/download/reports/>

110 Fayda National ID, Ethiopia. Official programme overview — foundational digital ID under Proclamation No. 1284/2023. <https://www.id.gov.et/>; World Bank. (2026, May 6). Ethiopia's Fayda results under the Global DPI Program. <https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program>

111 World Bank Restructures \$430m Digital ID Project For Nigeria <https://nationaleconomy.com/world-bank-restructures-430m-digital-id-project-for-nigeria/>

112 World Bank. (2026, January 28). Senegal Digital Economy Acceleration Project: Restructuring paper. <https://documents1.worldbank.org/curated/en/099013026050538641/pdf/P172524-9a862e0b-dfb7-46ab-8c90-3096cadd5e1a.pdf>;

113 World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>

114 Kenya's Huduma: Data commodification and government tyranny <https://www.aljazeera.com/opinions/2019/8/6/kenyas-huduma-data-commodification-and-government-tyranny>

115 CCTV cameras will watch over Egyptians in new high-tech capital <https://www.reuters.com/world/cctv-cameras-will-watch-over-egyptians-new-high-tech-capital-trfn-2023-01-04/>

116 Rise of smart city surveillance tech across Africa to spy on citizens <https://www.ids.ac.uk/news/smart-city-surveillance-tech-across-africa/>; African Governments are Using "Smart City" Systems to Monitor Dissent and Consolidate State Control <https://cipesa.org/2026/04/ai-african-governments-are-using-smart-city-systems-to-monitor-dissent-and-consolidate-state-control/>

and the Universal DPI Safeguards Framework make these questions central to accountability.¹¹⁷

Across Africa, electoral deadlines can intensify the same dependency risks because procurement must be completed against a fixed polling calendar. Late procurement, proprietary architecture, weak testing and unclear exit arrangements leave little time to correct defects before their effects on rights become difficult or impossible to remedy.¹¹⁸ The lesson for DPI deployment is to build procurement safeguards, audit access, continuity and supplier-exit planning into the system lifecycle rather than treating them as commercial details.

Technical leadership is not the same as human rights leadership. Nigeria, Ethiopia, Ghana, Kenya and Uganda are among the strongest on scale or integration, while South Africa and Kenya provide the evidence that independent institutions can slow, reshape or scrutinise rollout. Across all eleven countries, public human-rights due diligence by vendors and financiers remains a weak point.

4.2 Impact of DPI Systems on Human Rights, Inclusion and Access to Services

The deployment and integration of DPI reconfigures the distribution of power between states, commercial technology intermediaries and citizens. When evaluated closely, DPI does not function as a neutral administrative system, rather, it acts as a rights and power multiplier. This is because while technical interoperability, digital payment rails, and digital identity registries streamline service delivery, making digital credentials compulsory for essential services converts administrative infrastructure into a rights chokepoint for those who cannot enrol. This is evident when access to fundamental human, socio-economic and civic rights is legally or operationally conditioned upon successful real-time biometric verification or digital profile lookup within state-operated databases. When enrollment bottlenecks, biometric read errors, uncollected smart cards, or geographic digital divides occur, administrative friction then converts into a cascading multisystem exclusion. Benefits are therefore greatest for people who are already documented, connected and able to use digital channels. The risks are manifest where identity, connectivity or automated verification becomes an exclusive condition for a service or the exercise of a civic right.

4.2.1 Rights Fundamentally Affected by DPI Systems

DPI implementation consistently impacts five core clusters of rights, namely: privacy and personal data protection; equality and non-discrimination; socio-economic rights; freedom of expression, assembly and access to information; and political participation. Privacy rights can be affected where large scale centralised biometric identity databases and interoperable data exchange platforms in countries such as *GavaConnect* in Kenya, *Jokkoo/PINS* in Senegal, *TunXRoad* in Tunisia, *UGHub* in Uganda or *Zam-Connect* in Zambia, expand state legibility, heightening risks of unauthorised inter-agency data sharing, function creep and surveillance. Ghana's Supreme Court decision of 25 February 2026 in *Gorni v Vodafone Ghana Ltd and Others* is a recent example where the court treated unauthorised linking of a SIM and mobile-money account to a Ghana Card as a privacy violation for which damages were available.¹¹⁹

The right to equality and non-discrimination can be impacted where enrollment pre-requisites such as for birth certificates and parental documentation and biometric capture mechanisms systematically disadvantage manual labourers with worn fingerprints, older adults, persons with disabilities, refugees, rural, minority and border communities. When states condition public services without providing functional offline fallbacks, they institutionalise indirect administrative discrimination.

117 UNDP. (2026). How the DPG Standard and Universal DPI Safeguards Framework are charting a safe and inclusive digital future. <https://www.undp.org/digital/blog/how-dpg-standard-and-universal-dpi-safeguards-framework-are-charting-safe-and-inclusive-digital-future>; UNDP. (2024). Universal DPI Safeguards Framework: A guide to building safe and inclusive DPI for societies (updated 2025). <https://www.undp.org/publications/universal-safeguards-digital-public-infrastructure>; Office of the United Nations High Commissioner for Human Rights. (2011). Guiding principles on business and human rights. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

118 International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; International Foundation for Electoral Systems. (2023). Cybersecurity programming guide for electoral assistance. <https://www.ifes.org/sites/default/files/2023-06/Cybersecurity-Programming-Guide-USAID.pdf>

119 Supreme Court of Ghana. (2026, February 25). *Gorni v. Vodafone Ghana Ltd and others* (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>

Socio-economic rights can be affected when access to essential services such as public healthcare, social assistance grants, or financial services are tied to digital identity.¹²⁰ Also, technical or administrative verification failures could directly infringe upon these rights. Freedom of expression, assembly and access to information can be affected when mandatory ID-linked SIM registration removes anonymous online communication and enables state monitoring leading to self-censorship. Further, state-directed internet disruptions deployed during protests or elections such as have been witnessed in Ethiopia, Kenya, Senegal, and Uganda can disrupt digital payment and public service portals thus resulting in a whole-of-society denial of rights.¹²¹

The right to political participation is triggered as foundational identity databases are increasingly utilised as the root register for generating voter registers and authenticating voters at polling stations using various election technologies in most countries.¹²² Consequently, errors, omissions or arbitrary blocks in civil identity registries can automatically propagate into political disenfranchisement. Election technologies can widen access and transparency, but its failure or restriction of networks or the use of digital surveillance in political contexts can simultaneously affect privacy, expression, information, and ultimately the exercise of political rights.

4.2.2 Beneficiaries and those Excluded from DPI Systems

The benefits and adverse impacts of DPI expansion are unevenly distributed across socio-economic and demographic groups with consistent patterns across the countries studied. The primary beneficiaries are the urban, formally employed, digitally literate, digitally connected, already-documented, banked populations who tend to realise the immediate benefits first. These include faster document issuance, remote authentication, fewer in-person visits, instant retail payment transfers, single-window service access and reduced queuing burdens.

The at-risk populations that face systematic exclusion include rural residents, manual labourers, low-income users, older people, persons with disabilities, women, people with weak civil-registration records, internally displaced persons, stateless persons, migrants, refugees, minority and border communities.¹²³

South Africa and Ghana show that accessibility and additional service channels can reduce barriers, while Uganda, Kenya, and Nigeria illustrate how pre-existing documentation or biometric difficulties can be carried into digital systems.

A voter may be excluded not because an electoral authority made a direct decision, but because a birth, citizenship, address, identity or biometric record held by another agency is missing or wrong. The more services and democratic processes reuse a single foundational record, the more important universal documentation, assisted access and cross-system correction become.

Kenya provides unusually granular evidence of how pre-existing documentation inequality can shape digital and financial inclusion. The 2024 FinAccess Household Survey, published by the Kenya National Bureau of Statistics in December 2024, found that 9.9% of adults remained financially excluded. Among excluded adults, 51.5% cited lack of an identity card as a barrier, and rural youth accounted for 45.5% of the excluded population. Financial inclusion among persons with disabilities stood at 77.9%, below the national average of 84.8%.¹²⁴ These figures do not establish that DPI caused the exclusion. They show, however, that when identity becomes a reusable gateway to finance and public services, unresolved documentation barriers can be carried forward and amplified unless alternative access and rapid correction mechanisms are available.

4.2.3 Digital Identity, Data Exchange Systems and Access to Essential Services

Integration can reduce transaction costs and improve targeting, but it also increases the number of services affected by a failed identity or connectivity check. In Uganda, the High Court on 10 June 2025 dismissed *Initiative for Social and Economic Rights (ISER) and 2 others v The Attorney General and Another (Miscellaneous Cause No. 0086 of 2022) [2025] UGHCCD 90*, a challenge to the use of the National Identity Register and mandatory identification requirements in accessing social protection and public

¹²⁰ Biometric Update (2025). *Mandatory digital ID for banking policy goes into effect in Ethiopia*. 6 Jan 2025. Retrieved from <https://www.biometricupdate.com/202501/mandatory-digital-id-for-banking-policy-goes-into-effect-in-ethiopia>

¹²¹ OONI (Open Observatory of Network Interference) (2023). *Senegal: Social Media Blocks and Network Outages Amid Political Unrest*. Aug 2023. Retrieved from <https://ooni.org/post/2023-senegal-social-media-blocks>; CIPESA. (2024, September 27). 2024 State of Internet Freedom in Africa report unveils the promises and challenges of technology in African elections. https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf; ISS Africa (Institute for Security Studies) (2025). *Offline and silenced: Africa's quiet rise of internet repression*. Dec 2025. Retrieved from <https://issafrica.org/iss-today/offline-and-silenced-africa-s-quiet-rise-of-internet-repression>

¹²² International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>;

¹²³ Biometric Digital-ID in Africa: Progress and Challenges to Date – Ten Country 33 Case Studies https://paradigmhq.org/wp-content/uploads/2025/12/Biometric_Digital_ID_in_Africa.pdf?x2570

¹²⁴ Kenya National Bureau of Statistics. (2024, December). 2024 FinAccess household survey report. <https://www.knbs.or.ke/reports/2024-finaccess-household-survey-report/>

health services. The court held that the applicants had not proved systemic exclusion or discrimination arising from the National ID system, distinguishing the individual and operational difficulties presented in evidence from barriers inherent in the system. It upheld mandatory use of the National ID for Social Assistance Grants for Empowerment (SAGE) benefits as lawful and necessary for effective service delivery and found no legal or policy requirement making the National ID mandatory for access to public health services.¹²⁵

In Ethiopia, Fayda is already being connected to banks, Telebirr and other providers, and the National Bank of Ethiopia's 2026–2030 strategy sets a direction toward Fayda as the unique KYC identifier for all accounts and wallets by 2030.¹²⁶ Nigeria's identity harmonisation and SIM/financial linkages make the NIN increasingly important to communications and formal services.¹²⁷ In Ghana, the Ghana Card was the sole identity document for the 2022 SIM re-registration exercise, and the 2026 L.I. 2523 rules tightened the verification standard through mandatory biometric checks.¹²⁸

Civic participation is affected when the same systems support voter identification or when connectivity is restricted during an election.

Across Africa, voter registration and verification should be understood alongside health, finance, and social protection as rights-bearing public functions.¹²⁹ The difference is time. An authentication error in an ordinary service may be corrected days later; an unresolved voter-register or biometric error at a fixed election deadline may deny participation until the next electoral cycle. This makes rapid pre-election correction and election-day exception procedures substantive safeguards.

4.2.4 DPI Implementation and the Patterns of Inequality or Discrimination

DPI does not create most underlying inequalities, but it can reproduce or intensify them when unequal documentation, disability, gender, income, geography or language affect the ability to enrol, authenticate or seek correction. Kenya's long-running documentation barriers for Nubian, Somali and border communities, Uganda's exclusion litigation, and affordability or access constraints in South Africa, Zambia and Zimbabwe illustrate different forms of this problem. Ethiopia also demonstrates the value of targeted inclusion: Ethio Telecom reported registering more than four million farmers and 28,000 internally displaced persons during 2025/26.¹³⁰ These gains do not remove the need to measure who remains unable to enrol or authenticate.

Across Africa, these inequalities also shape who can participate safely in digital public life. Technology-facilitated gender-based violence, online harassment and misogynistic disinformation can deter women from political and civic participation even where formal digital access is improving. ACHPR Resolution 522 of 2022 calls for legal, research and awareness responses to digital violence against women.¹³¹ CIPESA reported in April 2025 that a Kenyan study found 90% of young adults in Nairobi tertiary institutions had experienced online gender-based violence, including 39% who reported direct victimisation.¹³² This is not evidence that DPI causes such violence, but it shows why an assessment of digital democracy cannot stop at connectivity or identity coverage.

¹²⁵ High Court of Uganda, Civil Division. (2025, June 10). Initiative for Social and Economic Rights (ISER) and 2 others v. Attorney General and another (Miscellaneous Cause No. 0086 of 2022) [2025] UGHCCD 90. <https://ulii.org/en/akn/ug/judgement/ughccd/2025/90/eng@2025-06-10>

¹²⁶ Fayda National ID, Ethiopia. (n.d.). Fayda ID strategy. Retrieved September 13, 2026, from <https://id.gov.et/strategies>; National Bank of Ethiopia. (2025, December 9). National Digital Payments Strategy 2026–2030 [Draft, released for consultation]. https://nbe.gov.et/wp-content/uploads/2025/12/Ethiopia_NDPS_Draft_E.pdf

¹²⁷ Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry–NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>; State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026-into-law-as-minister-reveals-the-arrest-of-terrorists-with-nimc-database/>

¹²⁸ National Communications Authority, Ghana. (2026, March 18). New SIM registration process and verification findings. <https://nca.org.gh/2026/03/18/nca-dg-assures-robust-consumer-centric-approach-to-new-sim-registration-process/>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory-for-ghana-card-verification-under-new-li-2523/>; National Communications Authority, Ghana. (2022, November 5). SIM registration using the voters' ID card: A clarification. <https://nca.org.gh/2022/11/06/sim-registration-using-the-voters-id-card-a-clarification/>; National Communications Authority, Ghana. (2022, September 5). Punitive measures for unregistered SIM cards kick in September 5. <https://nca.org.gh/2022/09/05/punitive-measures-for-unregistered-sim-cards-kick-in-september-5/>

¹²⁹ International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; African Commission on Human and Peoples' Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achprres655lxxxvi-2026>

¹³⁰ Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethiotelcom.et/2025-26-budget-year-annual-business-performance-report/5/>

¹³¹ African Commission on Human and Peoples' Rights. (2022, August 11). Resolution on the protection of women against digital violence in Africa (ACHPR/Res.522 (LXXII) 2022). <https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr>

¹³² CIPESA. (2025, April 25). Tackling the crisis of digital violence against women in Africa: Which way for ACHPR Resolution 522? <https://cipesa.org/2025/04/tfgbv/>

Political inequality requires separate treatment. In Tunisia, Human Rights Watch reported on 2 September 2026 that at least 20 associations had been suspended in waves during July–October 2025 and April–May 2026 amid a broader civic-space crack-down.¹³³ That is not evidence that DPI caused the suspensions. It is evidence about the environment in which biometric, data-exchange and digital-service systems are being governed, including the ability of civil society to scrutinise them.

4.2.5 Systemic Effects of the Interaction of Multiple DPI Pillars

The emerging trend is that when identity, data exchange, payments and connectivity are linked, a single error or state action can have consequences across several rights at once. Uganda provides a recent example of cumulative political risk. The national-ID framework supports voter administration and other services, and UCC suspended public internet and selected mobile services from 13 January 2026 during the general-election period, restoring public access on 18 January.¹³⁴ Ethiopia's ecosystem is also becoming more interconnected through Fayda, banking, Telebirr and government services.¹³⁵ Nigeria and Ghana link identity closely to communications and finance.¹³⁶

Across Africa, electoral convergence adds another possible dependency to this chain. The risk is not that every country already links identity, SIMs, payments and voter systems, but that the same credential and connectivity layer can increasingly mediate communication, finance, public services and political participation.¹³⁷ Common-mode failures and broad government access therefore become more consequential as the stack tightens.

The cumulative effect can also be beneficial. A verified identity can reduce repeated documentation; interoperable payments can expand financial participation; and a well-governed data exchange layer can reduce the need for citizens to submit the same information repeatedly. The policy challenge is to make correction, appeal, purpose limitation, access logs and alternative channels transcend the stack as effectively as data does.

4.2.6 Cross-cutting Progress and Continuing Challenges

Overall, the evidence is mixed rather than uniformly rights-reducing. South Africa's widening Smart ID service network,¹³⁸ Ghana's payment interoperability,¹³⁹ Ethiopia's targeted enrolment of farmers and internally displaced people,¹⁴⁰ and Zambia's emphasis on inclusive digital access under DZAP¹⁴¹ are progressive markers. The main areas needing change are the use of single credentials as mandatory gateways, weak correction and appeal systems, limited public audit evidence, and uneven protection of connectivity during politically sensitive periods.

Across Africa, election administration has shown relative progress. Ghana retained alternative routes to voter registration in 2024.¹⁴² Ethiopia retained manual registration alongside Fayda-enabled digital registration in 2026.¹⁴³ Kenya and South Africa

- 133 Human Rights Watch. (2026, September 2). Tunisia: Civil society under siege. <https://www.hrw.org/news/2026/09/02/tunisia-civil-society-under-siege>
- 134 Uganda Communications Commission. (2026, January 14). Temporary suspension of public internet access and selected mobile services. <https://www.ucc.co.ug/wp-content/uploads/2026/01/Temporary-suspension-of-public-internet-access-and-mobile-services.pdf>; Uganda Communications Commission. (2026, January 18). Public update: Restoration of public internet access. <https://www.ucc.co.ug/public-update-18th-january-2026-press-briefing-to-update-the-country/>
- 135 Fayda National ID, Ethiopia. (n.d.). Fayda ID strategy. Retrieved September 13, 2026, from <https://id.gov.et/strategies>
- 136 Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry–NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory-for-ghana-card-verification-under-new-l-i-2523/>
- 137 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>
- 138 SANews. (2026, June 24). More than 200 bank branches now offering Smart ID card. <https://www.sanews.gov.za/south-africa/more-200-bank-branches-now-offering-smart-id-card>
- 139 Ghana Interbank Payment and Settlement Systems. (2026). Industry performance: 2025 transaction volume and value. <https://ghipss.net/component/content/category/56-newsletters>
- 140 Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethiotelcom.et/2025-26-budget-year-annual-business-performance-report/5/>
- 141 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>
- 142 Ghana News Agency. (2024, March 7). Election 2024: EC shelves use of Ghana Card as sole identity document. <https://gna.org.gh/2024/03/election-2024-ec-shelves-use-of-ghana-card-as-sole-identity-document/>
- 143 Intergovernmental Authority on Development. (2026, June 3). IGAD Election Observation Mission to Ethiopia's 7th General Election: Preliminary report. <https://igad.int/igad-election-observation-mission-to-the-7th-general-election-of-the-federal-democratic-republic-of-ethiopia-held-on-monday-june-1-2026-preliminary-report/>

preserved paper/manual voter verification when devices failed.¹⁴⁴ These are important because resilience and inclusion can be designed into digitisation rather than being added after failure.

The right picture across the 11 countries is more differentiated. In Egypt¹⁴⁵ and Tunisia,¹⁴⁶ the central concern is the interaction between increasing state data capacity and constrained civic scrutiny. Although Tunisia's Unique Citizen Identifier framework includes a potentially progressive transparency feature where citizens can request information about the public bodies that have used their identifier.¹⁴⁷ In Ethiopia,¹⁴⁸ Uganda¹⁴⁹ and Kenya,¹⁵⁰ access and political equality are more directly shaped by whether people can obtain, authenticate, and correct foundational identity records, with the consequences increasing as identity is linked to banking, taxation, social protection, telecommunications or elections.

Ghana, Nigeria and Senegal show that gains in service delivery and risks to rights often co-exist in the same system. Ghana's mature payments and identity verification reduce transaction friction, yet the 2022 SIM-registration exercise and the 2026 Gorni case demonstrate that access and privacy cannot be assumed from scale alone.¹⁵¹ Nigeria's NIN and payment ecosystem broadens formal access but makes identity-data governance and correction more consequential.¹⁵² Senegal's digital modernisation can simplify services, but the 2023 shutdowns and the ECOWAS Court's 14 May 2025 judgement show how control of connectivity can affect expression, information and work independently of whether the underlying DPI systems are technically sound.¹⁵³

South Africa, Zambia and Zimbabwe show a different balance. South Africa has documented gains from wider Smart ID access and payment modernisation, but access remains conditioned by affordability, literacy, documentation and frontline state capacity.¹⁵⁴ Zambia's digital-access programme and payment systems offer opportunities for more efficient services, while incomplete

- 144 Independent Electoral and Boundaries Commission, Kenya. (2022). Post-election evaluation / register of voters report. <https://www.iebc.or.ke/uploads/resources/pabjKTV6Xa.pdf>; Electoral Commission of South Africa. (2024). 2024 national and provincial elections report. <https://www.elections.org.za/content/Documents/Election-reports/National-and-Provincial-Elections/2024-National-and-Provincial-Elections-Report/>
- 145 State Information Service, Egypt. (2026, July 21). Communications Minister: Egypt to offer more than 270 digital government services by end-2026. <https://sis.gov.eg/en/media-center/news/communications-minister-egypt-to-offer-more-than-270-digital-government-services-by-end-2026/>
- 146 Human Rights Watch. (2026, September 2). Tunisia: Civil society under siege. <https://www.hrw.org/news/2026/09/02/tunisia-civil-society-under-siege>
- 147 Tunisia Legal Database / DCAF. (2020, May 12). Decree-Law No. 2020-17 on the Unique Citizen Identifier. <https://legislation-securite.tn/latest-laws/decret-loi-du-chef-du-gouvernement-n-2020-17-du-12-mai-2020-relatif-a-lidentifiant-unique-du-citoyen/>
- 148 Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethiotelecom.et/2025-26-budget-year-annual-business-performance-report/5/>; Fayda National ID, Ethiopia. (n.d.). Fayda ID strategy. Retrieved September 13, 2026, from <https://id.gov.et/strategies>
- 149 High Court of Uganda, Civil Division. (2025, June 10). Initiative for Social and Economic Rights (ISER) and 2 others v. Attorney General and another (Miscellaneous Cause No. 0086 of 2022) [2025] UGHCCD 90. <https://ulii.org/en/akn/ug/judgement/ughccd/2025/90/eng@2025-06-10>
- 150 Kenyalaw. (2024, August 12). Haki na Sheria Initiative v. Attorney General & 4 others [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>; Directorate of Immigration Services, Kenya. (2024, September 19). Issuance of Maisha Card IDs. <https://immigration.go.ke/issuance-of-maisha-card-ids/>
- 151 Supreme Court of Ghana. (2026, February 25). Gorni v. Vodafone Ghana Ltd and others (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>; Ghana Interbank Payment and Settlement Systems. (2026). Industry performance: 2025 transaction volume and value. <https://ghipss.net/component/content/category/56-newsletters>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory-for-ghana-card-verification-under-new-l-i-2523/>; National Communications Authority, Ghana. (2022, November 5). SIM registration using the voters' ID card: A clarification. <https://nca.org.gh/2022/11/06/sim-registration-using-the-voters-id-card-a-clarification/>; National Communications Authority, Ghana. (2022, September 5). Punitive measures for unregistered SIM cards kick in on September 5. <https://nca.org.gh/2022/09/05/punitive-measures-for-unregistered-sim-cards-kick-in-september-5/>
- 152 Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry-NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>; State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026-into-law-as-minister-reveals-the-arrest-of-terrorists-with-nimc-database/>
67. Nigeria Inter-Bank Settlement System. (2025, June 23). NIBSS unveils the National Payment Stack to power the future of instant payments in Nigeria. <https://nibss-plc.com.ng/nibss-unveils-the-national-payment-stack-to-power-the-future-of-instant-payments-in-nigeria/>
- 153 OONI (Open Observatory of Network Interference). (2023, August). Senegal: Social media blocks and network outages amid political unrest. <https://ooni.org/post/2023-senegal-social-media-blocks>; Human Rights Watch. (2023, August 1). Senegalese government dissolves opposition party, cuts internet. <https://www.hrw.org/news/2023/08/01/senegalese-government-dissolves-opposition-party-cuts-internet>; Community Court of Justice, ECOWAS. (2025, May 14). L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JUD-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-LINFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>; Ministry of Communication, Telecommunications and the Digital Economy, Senegal / Jokkoo. (2026, January 16). Inter-ministerial and interoperable data-exchange platform of Senegal. <https://pins.sn/actualites/2026-01/plateforme-interministerielle-et-interoperable-dechange-de-donnees-du-senegal>
- 154 Government of South Africa / MyMzansi. (2025, May). Roadmap for the digital transformation of government. https://www.mymzansi.gov.za/static/resources/MyMzansi_Roadmap_Final_2025.pdf; SANews. (2026, June 24). More than 200 bank branches now offering Smart ID card. <https://www.sanews.gov.za/south-africa/more-200-bank-branches-now-offering-smart-id-card>

integration and contested interception powers create different inclusion and privacy questions.¹⁵⁵ Zimbabwe's more fragmented digital-government environment means some cascading cross-system risks are less immediate than in highly integrated systems, but fragmentation creates its own coordination problems and the proposed Project Pangolin data layer could change that risk profile in the next five years.¹⁵⁶

Across the sample, the strongest progress indicator is not simply greater enrollment. It is evidence that people who would otherwise face distance, cost, fraud or repeated paperwork can actually use services more easily without losing practical alternatives or control over their data. On the flip side, the strongest warning sign is that a single identity or connectivity failure could become the point at which several social, economic and political rights are simultaneously denied.

South Africa provides the strongest positive rights dividend, although it remains incomplete. Ghana, Kenya, Nigeria, Senegal, Zambia and Zimbabwe show mixed outcomes in which service gains coexist with exclusion or governance risks. Ethiopia, Uganda and Egypt present the highest systemic risk because extensive state digital capacity intersects with mandatory use, conflict, security institutions or restrictive civic space. These are contextual judgements, not claims that every DPI component in those countries causes rights violations.

4.2 Regulatory and Institutional Frameworks Governing DPI in Africa

Legal, regulatory, and institutional frameworks have expanded considerably, but this does not mean that safeguards are operational or that institutions are independent and capable of constraining high-impact systems. Across the 11 countries, progress in law and court decisions sit alongside continuing gaps in implementation, resources, institutional independence and DPI-specific oversight.

4.2.1 Legal and Regulatory Frameworks Governing DPI

Results show that countries do not rely on a single law or policy; instead, the legal and institutional framework varies according to the DPI system concerned, with civil registration and identity, telecommunications, digital payments, taxation and other digital public systems operating under their respective sectoral mandates.

In Ethiopia, Article 5 of Proclamation No. 1284/2023 provides that the Council of Ministers may establish an institution to implement the digital identification system, or that the function may be housed in an existing government body. In Uganda, DPI is primarily governed by the Registration of Persons Act (ROPA), which establishes the legal foundation for Uganda's foundational identity infrastructure. The Act gives the National Identification and Registration Authority (NIRA) powers to register persons, issue national identification numbers and cards, maintain the Register, and harmonise information from other government databases. Other laws include the National Information Technology Authority, Uganda Act establishes the National Information Technology Authority-Uganda (NITA-U) as an autonomous statutory body responsible for coordinating, promoting, and monitoring information technology development in Uganda; the National Payment Systems Act provides the legal framework for payment systems. The Act gives the Bank of Uganda a central supervisory role, including overseeing payment systems for safety and efficiency and empowering it to regulate the entry and conduct of participants, issue directives and guidelines, require changes to payment-system rules, and suspend systems where necessary.

In Ghana, under Regulation 7 of Legislative Instrument (L.I. 2111), the Ghana Card is mandatory for access to a wide range of services, including banking, credit, taxes, SIM registration, public services such as the National Health Insurance Scheme (NHIS), driver's licenses, pension schemes, and voter registration. Like other study countries, the Constitution of Kenya 2010 provides the foundational protections engaged by DPI: privacy, equality, human dignity, and access to information.¹⁵⁷ The principal legislative framework is the Data Protection Act 2019, supplemented by the Computer Misuse and Cybercrimes Act and registration

¹⁵⁵ World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>; National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>

¹⁵⁶ World Bank. (2021). Digital economy for Zimbabwe: Country diagnostic report. <https://documents1.worldbank.org/curated/en/982981621880260112/pdf/Digital-Economy-for-Zimbabwe-Country-Diagnostic-Report.pdf>; United Nations in Zimbabwe. (2026, March 14). Zimbabwe unveils 2026–2030 AI strategy to advance inclusive digital transformation. <https://zimbabwe.un.org/en/311859-zimbabwe-unveils-2026%E2%80%932030-ai-strategy-advance-inclusive-digital-transformation>; Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. https://zimtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE_2026-National-Budget_25_November_2025-final.pdf

¹⁵⁷ Constitution of Kenya 2010, arts 27 (equality and freedom from discrimination), 28 (human dignity), 31 (privacy) and 35 (access to information).

statutes governing identity systems.¹⁵⁸

In Nigeria, DPI governance operates through a fragmented framework comprising the National Information Technology Development Agency (NITDA) Act 2007,¹⁵⁹ the National Digital Economy Policy and Strategy 2020–2030, the Nigeria e-Government Interoperability Framework,¹⁶⁰ Nigeria Data Protection Act,¹⁶¹ the Cybercrimes Act 2015 (as amended)¹⁶² and sector-specific regulations. The proposed National Digital Economy and E-Governance Bill 2025 represents an attempt to establish a more comprehensive statutory framework for digital governance and digital service delivery but is yet to be enacted into law.¹⁶³

In Zimbabwe, the Declaration of Rights within the Constitution provides safeguards relevant to the DPI systems. These include the right to privacy under section 57, equality and non-discrimination under section 56, access to information under section 62, and citizenship rights relating to passports, birth certificates, and other identity documents under section 35. These protections provide the broader human-rights framework within which digital identity, data processing and digital public service systems should operate. In addition, the Cyber and Data Protection Act provides the principal statutory framework governing the processing and protection of personal data across these systems.

Tunisia's DPI ecosystem is governed by a fragmented set of laws, decrees, ministerial instruments, institutional arrangements and privacy policies. The principal legal foundation remains Organic Law No. 63-2004 on personal data protection, supplemented by system-specific instruments. The IUC is governed by Decree-Law No. 2020-17 and Decree No. 2020-312, while electronic data exchange and interoperability are regulated through Decree-Law No. 2020-31 and Order No. 777-2020. Mobile ID was launched through Ministerial Circular No. 007 of 20 June 2022, supported indirectly by the IUC and interoperability framework. The future biometric national identity card is governed by Organic Law No. 2024-22, which amends the existing CIN legislation and provides for biometric data, an electronic chip, authentication and electronic signatures.

All 11 countries now have relevant data-protection or privacy rules, but their age, scope and operational status differ. Egypt's Personal Data Protection Law No. 151 of 2020 was operationalised by Executive Regulations No. 816 of 2025, effective 2 November 2025.¹⁶⁴ Ethiopia's Digital Identification Proclamation No. 1284/2023 provides the legal basis for Fayda, and the Personal Data Protection Proclamation No. 1321/2024, dated 24 July 2024, established the newer data-protection framework.¹⁶⁵ Ghana applies the Data Protection Act, 2012 (Act 843);¹⁶⁶ Kenya the Data Protection Act, 2019 (No. 24 of 2019);¹⁶⁷ and Nigeria the Nigeria Data Protection Act, 2023, alongside the National Identity Management Commission Act, 2026, signed on 26 June 2026.¹⁶⁸

Across Africa, electoral law, identity law and data-protection law still tend to evolve in separate silos even as the underlying systems converge. This creates uncertainty about controller roles, attributes exchanged, retention, audit rights and correction when an EMB queries or imports foundational data. A rights-respecting linkage therefore needs an explicit legal basis and institutional boundary, not only a technically secure API.

Senegal's principal personal-data law is Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data.¹⁶⁹ South Africa applies the Protection of Personal Information Act 4 of 2013 (POPIA), which came fully into force on 1 July 2021.¹⁷⁰ Tunisia re-

¹⁵⁸ Data Protection Act 2019 (Kenya), No 24 of 2019; Computer Misuse and Cybercrimes Act 2018 (Kenya); Registration of Persons Act (Kenya) (as amended to establish NIIMS).

¹⁵⁹ NITDA Act, <https://nitda.gov.ng/nitda-act/> accessed August 31, 2026.

¹⁶⁰ National Information Technology Development Agency (NITDA), <https://nitda.gov.ng/regulations/> accessed August 31, 2026.

¹⁶¹ Nigeria data Protection Act, <https://ndpc.gov.ng/resources/> accessed August 31, 2026.

¹⁶² which regulates aspects of cybersecurity and digital activities

¹⁶³ Placbillstrack, HB 1599: National Digital Economy and E-Governance Bill, 2024, <https://p.placbillstrack.org/bills/9a4f67d4-6968-4082-801c-91f3cbcdc955/> accessed August 31, 2026.

¹⁶⁴ Personal Data Protection Center, Egypt. (2026). Legal framework: Personal Data Protection Law No. 151 of 2020 and Executive Regulations No. 816 of 2025. <https://www.pdpc.gov.eg/>; Shand Partners. (2026, January 11). Executive regulations of the data protection law in Egypt (Law No. 151 of 2020). <https://www.shand-partners.com/insights/briefings/telecoms-media-technology/the-issuance-of-the-executive-regulations-of-the-data-protection-law-and-the-establishment-of-the-data-protection-centre/>

¹⁶⁵ Ministry of Justice, Ethiopia. (2024, July 24). Personal Data Protection Proclamation No. 1321/2024. <https://justice.gov.et/en/law/personal-data-protection-proclamation/>; Fayda National ID, Ethiopia. (n.d.). Fayda ID strategy. Retrieved September 13, 2026, from <https://id.gov.et/strategies>

¹⁶⁶ Ghana Legal Information Institute / Data Protection Commission. (2012, May 10). Data Protection Act, 2012 (Act 843). <https://ghalii.org/akn/gh/act/2012/843/eng@2012-05-18>

¹⁶⁷ Kenya Law. (2019). Data Protection Act, 2019 (No. 24 of 2019). <https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2019-11-15>

¹⁶⁸ Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act, 2023. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf

¹⁶⁹ Commission de Protection des Données Personnelles, Senegal. (2008). Law No. 2008-12 of 25 January 2008 on the protection of personal data. <https://www.cdp.sn/legislation/textes-legislatifs>

¹⁷⁰ Government of South Africa. (2013). Protection of Personal Information Act 4 of 2013 (POPIA). <https://www.gov.za/documents/protection-personal-infor->

lies principally on Organic Law No. 2004-63 of 27 July 2004 on the Protection of Personal Data, while Organic Law No. 2024-22 amended the national identity-card framework to provide for biometric capture and an electronic credential.¹⁷¹ Uganda applies the Data Protection and Privacy Act, Chapter 97 (enacted in 2019), and the Data Protection and Privacy Regulations, 2021.¹⁷² Zambia has the Data Protection Act No. 3 of 2021 and the Electronic Government Act No. 41 of 2021,¹⁷³ and Zimbabwe has the Cyber and Data Protection Act, 2021 in force from 11 March 2022.¹⁷⁴

4.2.2 Oversight, Accountability, and Institutional Responsibilities

The research findings show that transparency and accountability remain strongest where implementing agencies such as Data Protection Authorities are empowered with oversight powers, such as investigating compliance and remedial measures in the implementation of PDI systems. South Africa's Information Regulator, Kenya's courts,¹⁷⁵ and the Office of the Data Protection Commissioner, Nigeria's Data Protection Commission, Ghana's Data Protection Commission,¹⁷⁶ and the ECOWAS Court route available to West African states¹⁷⁷ provide different forms of external oversight. For example, on 3 July 2023, South Africa's regulator, for example, issued an infringement notice and a R5 million administrative fine against the Department of Justice and Constitutional Development for non-compliance with an earlier POPIA enforcement notice.¹⁷⁸

The same principle applies to election-related DPI. Electoral-management bodies need practical and formal independence, while data-protection authorities need authority to supervise personal-data processing without taking over the EMB's constitutional mandate. Also, shared infrastructure should not create an informal chain in which an executive identity or digital-government agency can determine electoral eligibility or system availability without independent checks.¹⁷⁹

The position is more difficult where oversight is fragmented, dependent, or only recently activated. Egypt's Personal Data Protection Center is now operating under the 2025 Executive Regulations, an important change from the earlier dormant-law position, but its institutional location within the Ministry of Communications and Information Technology raises questions as to whether it can act with independence and impartiality.¹⁸⁰ Ethiopia's Personal Data Protection Proclamation No. 1321/2024 is recent and assigns supervisory functions within the existing communications-regulatory architecture rather than creating the independent

mation-act

¹⁷¹ Tunisia Legal Database / DCAF. (2024, March 11). Organic Law No. 2024-22 amending Law No. 93-27 on the National Identity Card. <https://legislation-securite.tn/latest-laws/loi-organique-n-2024-22-du-11-mars-2024-modifiant-et-completant-la-loi-n-93-27-du-22-mars-1993-relative-a-la-carte-nationale-didentite/>; Tunisia Legal Database / DCAF. (2004, July 27). Organic Law No. 2004-63 on the protection of personal data. <https://legislation-securite.tn/latest-laws/loi-organique-n-2004-63-du-27-juillet-2004-portant-sur-la-protection-des-donnees-a-caractere-personnel/>; Tunisia Legal Database / DCAF. (2004, July 27). Organic Law No. 2004-63 on the protection of personal data. <https://legislation-securite.tn/latest-laws/loi-organique-n-2004-63-du-27-juillet-2004-portant-sur-la-protection-des-donnees-a-caractere-personnel/>

¹⁷² Uganda Legal Information Institute. (2019). Data Protection and Privacy Act, 2019. <https://ulii.org/en/akn/ug/act/2019/9/eng@2019-05-03>; Uganda Legal Information Institute. (2021, March 12). Data Protection and Privacy Regulations, 2021 (S.I. No. 21 of 2021). <https://ulii.org/en/akn/ug/act/si/2021/21/eng@2021-03-12>

¹⁷³ National Assembly of Zambia. (2021). The Data Protection Act, 2021. <https://www.parliament.gov.zm/node/8853>

¹⁷⁴ Zimbabwe Legal Information Institute. (2022, March 11). Cyber and Data Protection Act, 2021 (Chapter 12:07). <https://zimlii.org/akn/zw/act/2021/5/eng@2022-03-11>

¹⁷⁵ Kenyalaw. (2024, August 12). Haki na Sheria Initiative v. Attorney General & 4 others [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>

¹⁷⁶ Supreme Court of Ghana. (2026, February 25). Gorni v. Vodafone Ghana Ltd and others (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>

¹⁷⁷ Community Court of Justice, ECOWAS. (2025, May 14). L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JUD-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-LINFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>

¹⁷⁸ Information Regulator of South Africa. (2023, July 4). Infringement notice and R5 million administrative fine issued to the Department of Justice and Constitutional Development for contravention of POPIA. <https://infoeregulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGMENT-NOTICE-IS-SUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf>

¹⁷⁹ International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>

¹⁸⁰ Shand Partners. (2026, January 11). Executive regulations of the data protection law in Egypt (Law No. 151 of 2020). <https://www.shandpartners.com/insights/briefings/telecoms-media-technology/the-issuance-of-the-executive-regulations-of-the-data-protection-law-and-the-establishment-of-the-data-protection-centre/>

commission originally envisaged in some project documents.¹⁸¹ Uganda¹⁸² and Zambia¹⁸³ divide responsibility across identity, data-protection, communications, payment and cybersecurity regulatory bodies. Zimbabwe's Cyber and Data Protection Act designates POTRAZ, the telecommunications regulator, as the Data Protection Authority, while the Civil Registry Department is responsible for issuance of identity documents.¹⁸⁴ These arrangements do not by themselves prove weak enforcement, but they make institutional independence and coordination central to the assessment.

4.2.3 Implementation of Safeguards

The gap between law on paper and law in use remains substantial; however, there are several concrete examples of safeguards being enforced in the past three years. In Kenya, the High Court's 30 January 2020 judgment in *Nubian Rights Forum & 2 others v Attorney General & 6 others* permitted NIIMS to proceed only after an appropriate and comprehensive regulatory framework was enacted, and later Maisha Namba litigation continued to test privacy and impact-assessment duties.¹⁸⁵ On 16 January 2024, the Gauteng High Court in *P.P.M. and Others v Minister of Home Affairs and Others* held unlawful and unconstitutional the Department of Home Affairs' practice of automatically blocking identity numbers suspected of fraud or irregularity before investigations had been concluded and without fair administrative process.¹⁸⁶ The Court determined that the practice could prevent affected individuals from accessing banking, social grants, travel documents and other services requiring identity verification. The court was decisive on procedural safeguards and ordered specific protections for children affected by the blocking of their own or their parents' identity numbers.

On 14 May 2025, the ECOWAS Community Court of Justice in *L'Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) and Ndiaga Gueye v Republic of Senegal* held Senegal's June–July 2023 internet and social-media restrictions unlawful and awarded compensation for violations of expression, access to information and, for Gueye, the right to work.¹⁸⁷ On 25 February 2026, Ghana's Supreme Court in *Gorni v Vodafone Ghana Ltd and Others* awarded a privacy remedy for unauthorised Ghana Card-linked SIM/mobile-money use.¹⁸⁸ On 17 March 2026, Uganda's Constitutional Court in *Alternative Digitalk Limited and Others v Attorney General* invalidated the Computer Misuse (Amendment) Act after finding that Parliament had passed it without the Speaker ascertaining the constitutionally required quorum. The Court permanently restrained government agencies from enforcing the affected provisions of the Computer Misuse (Amendment) Act,¹⁸⁹ and the Attorney General subsequently directed prosecuting and law enforcement agencies to halt new arrests and prosecutions and terminate pending proceedings under them.¹⁹⁰

Across Africa, election technology demonstrates that fallback, testing, and incident response are forms of implementation rather than secondary technical detail. A legal right to vote is not protected by a biometric-verification rule unless officials know when and how to use an exception path, devices are stress-tested, and incidents are disclosed quickly enough to preserve partici-

181 Ministry of Justice, Ethiopia. (2024, July 24). Personal Data Protection Proclamation No. 1321/2024. <https://justice.gov.et/en/law/personal-data-protection-proclamation/>

182 Uganda Legal Information Institute. (2019). Data Protection and Privacy Act, 2019. <https://ulii.org/en/akn/ug/act/2019/9/eng@2019-05-03>; National Identification and Registration Authority, Uganda. (2025, May 15). Press statement on the mass enrolment exercise. <https://www.nira.go.ug/publications/press-statement-on-the-mass-enrolment-exercise>

183 National Assembly of Zambia. (2021). The Data Protection Act, 2021. <https://www.parliament.gov.zm/node/8853>; National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>; National Assembly of Zambia. (2021). Electronic Government Act, No. 41 of 2021. <https://www.parliament.gov.zm/node/9014>

184 Zimbabwe Legal Information Institute. (2022, March 11). Cyber and Data Protection Act, 2021 (Chapter 12:07). <https://zimlii.org/akn/zw/act/2021/5/eng@2022-03-11>

185 Kenyalaw. (2024, August 12). Haki na Sheria Initiative v. Attorney General & 4 others [2024] KEHC 10021 (KLR). [https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024A biometric-verification rule does not protect a legal right to vote-08-12](https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024A%20biometric-verification%20rule%20does%20not%20protect%20a%20legal%20right%20to%20vote-08-12); High Court of Kenya. (2020, January 30). *Nubian Rights Forum & 2 others v. Attorney General & 6 others*; *Child Welfare Society shows that fallback, testing, and incident response are implementation choices rather than secondary technical details* & 8 others (Interested Parties) (Petition 56, 58 & 59 of 2019, Consolidated) [2020] KEHC 8772 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2020/8772>

186 High Court of South Africa, Gauteng Division. (2024, January 16). *P.P.M. and others v. Minister of Home Affairs and others* (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>

187 Community Court of Justice, ECOWAS. (2025, May 14). *L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal* (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JUD-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-L'INFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>

188 Supreme Court of Ghana. (2026, February 25). *Gorni v. Vodafone Ghana Ltd and others* (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>

189 Constitutional Court of Uganda. (2026, March 17). *Alternative Digitalk Limited and others v. Attorney General* (Consolidated Constitutional Petitions No. 34, 37 & 42 of 2022) [2026] UGCC 3. Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/judgement/ugcc/2026/3/eng@2026-03-17>

190 Anthony Wesaka, "AG halts arrests based on nullified Computer Misuse Law, Daily Monitor," Tuesday, March 26, 2026, <https://www.monitor.co.ug/uganda/news/national/ag-halts-arrests-based-on-nullified-computer-misuse-law-5403596>

pation. The 2026 Ugandan BVVK difficulties and the routine use of complementary manual records in Kenya and South Africa illustrate the point.¹⁹¹

Kenya also provides a more progressive sector-specific counterexample. Under the Digital Health Act, 2023 and the Digital Health (Data Exchange Component) Regulations, 2025, digital health systems operate within an explicit interoperability and data-governance framework.¹⁹² Related 2025 health-information regulations require certification applicants to provide evidence of registration with the Office of the Data Protection Commissioner, a Data Protection Impact Assessment report, security and privacy policies and a cybersecurity assessment; the data-exchange rules require purpose limitation, access controls and logging of requests. These requirements do not resolve wider DPI-governance gaps, but they show how rights and security controls can be embedded in an operational exchange regime rather than left only to general principles.

4.2.4 From Legal Safeguards to Practice: Persistent Governance Gaps

The most persistent gaps emerge where formal legal safeguards fail to translate into effective constraints on high impact DPI systems. Across the study countries, these gaps include broad national security exemptions in identity and data protection laws; limited use or publication of human rights and data protection impact assessment before systems are scaled; weak public auditability; inadequate cross-system correction, and remedy; opaque data-sharing and procurement arrangements; and limited independent oversight of national-security access to DPI systems.

Privacy and data protection guarantees are systematically undermined by broad and sweeping national security exemptions. In Ghana, Section 49 of the NIA Act permits data access without consent for national security.¹⁹³ In Ethiopia, article 53 of Proclamation 1321/2024 contains broad public-interest exemptions that carve out national security processing from DPA oversight.¹⁹⁴ In Kenya, under section 51(b) of the Data Protection Act and regulation 54 of the Data Protection (General) Regulations, 2021, processing of personal data for national security is exempted from certain compliance principles.¹⁹⁵ The issue is therefore not only whether safeguards exist, but whether privacy, cybersecurity and interception powers are coordinated under independent and reviewable rules.

Another category of gaps relates to opaque procurement, vendor dependency and missing DPIAs. Across the countries, governments do not proactively publish pre-deployment DPIAs, HRIAs, or vendor procurement contracts. Kenya's Data Protection Act, 2019 and its DPIA requirement were only made meaningful through litigation over Huduma Namba and Maisha Namba, beginning with the High Court's 30 January 2020 NIIMS judgement and continuing through later litigation.¹⁹⁶ In Ghana, public information on the Ghana Card, Ghana.gov and the emerging data-exchange layer is much stronger on system purpose and verification rules than on published DPI-specific impact assessments and audit outcomes.¹⁹⁷ Further, details of the 2018 NIA, Identity Management Systems (IMS), a subsidiary of the Margins Group public private partnership contract for the development of the Ghana Card remain confidential and with only some details made public.¹⁹⁸

In Ethiopia, publicly available documentation surrounding MOSIP and Tech5 hardware lacks a public DPIA, although it has adopt-

¹⁹¹ Independent Electoral and Boundaries Commission, Kenya. (2022). Post-election evaluation / register of voters report. <https://www.iebc.or.ke/uploads/resources/pabjKTV6Xa.pdf>; Electoral Commission of South Africa. (2024). 2024 national and provincial elections report. <https://www.elections.org.za/content/Documents/Election-reports/National-and-Provincial-Elections/2024-National-and-Provincial-Elections-Report/>; Electoral Commission of Uganda. (2026, January 15).

¹⁹² Kenya Law. (2023). Digital Health Act, 2023 (No. 15 of 2023). <https://new.kenyalaw.org/akn/ke/act/2023/15/eng@2023-11-24>; Kenya Law. (2025, April 11). Digital Health (Data Exchange Component) Regulations, 2025 (Legal Notice No. 77 of 2025). <https://new.kenyalaw.org/akn/ke/act/lv/2025/77/eng@2025-04-11/>

¹⁹³ National Identity Register Act, 2008 Act 750 <https://nca.org.gh/wp-content/uploads/2020/09/National-Identity-Register-Act-2008-750.pdf>

¹⁹⁴ Proclamation No. 1321/2024 Proclamation To Provide For Personal Data Protection https://www.dataguidance.com/sites/default/files/personal_data_protection_proclamation_1321-2024.pdf

¹⁹⁵ Data Protection (General) Regulations, 2021 <https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf>; Data Protection Act, <https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf>

¹⁹⁶ Kenyalaw. (2024, August 12). Haki na Sheria Initiative v. Attorney General & 4 others [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>; High Court of Kenya. (2020, January 30). Nubian Rights Forum & 2 others v. Attorney General & 6 others; Child Welfare Society & 8 others (Interested Parties) (Petition 56, 58 & 59 of 2019, Consolidated) [2020] KEHC 8772 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/>

¹⁹⁷ National Information Technology Agency, Ghana. (2025). Data Harmonisation Bill: Proposed National Data Exchange Platform and interoperability framework. <https://nita.gov.gh/wp-content/uploads/2025/NITA-Data-Harmonisation-Bill.pdf>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory>

¹⁹⁸ Cost Of The Ghana Card Project Is \$124 Million: Reaction To Minority Leader's Demand For Forensic Audit Of Nia Contract <https://nia.gov.gh/cost-of-gha->

ed the Digital Impact Alliance (DIAL) Digital ID Assessment framework.¹⁹⁹ The strategic cooperation agreement signed in 2018 between the government of Zimbabwe and Guangzhou-based Chinese AI firm CloudWalk Technology established a pipeline where domestic biometric data is shared to train AI models.²⁰⁰ In Uganda, NIRA publishes registration guidance and a data-protection policy, while the public record remains thin on a completed, system-wide impact assessment for the 2025–2026 mass renewal and on correction outcomes across linked services.²⁰¹

In Zimbabwe, the World Bank's 2021 digital-economy diagnostic documented fragmented government systems and limited interoperability, while later policy points toward greater integration; public detail on how future cross-agency access will be logged, audited and remedied remains limited.²⁰² Authentication capability is developing faster than public verifiability. The recurring gap is not only whether a system can recognise a person, but whether parties, observers, regulators, courts and citizens can understand system rules, inspect logs or results where lawful, distinguish technical failure from manipulation, and reconstruct what happened after an incident.²⁰³ That is as much a rule-of-law problem as a cybersecurity problem.

North Africa demonstrates the importance of the dates on which a law is enacted and when it becomes enforceable. Egypt enacted the Personal Data Protection Law No. 151 of 2020 but only operationalised it through Executive Regulations No. 816 of 2025, effective 2 November 2025, with the main compliance transition running into November 2026.²⁰⁴ Tunisia, by contrast, still relies principally on Organic Law No. 2004-63 of 27 July 2004 while new biometric and interoperability systems continue to develop.²⁰⁵ Egypt is therefore improving from a dormant baseline, while Tunisia's challenge is that an older framework is being asked to govern a newer and more interconnected environment.

Ethiopia's Digital Identification Proclamation No. 1284/2023 and Personal Data Protection Proclamation No. 1321/2024 establish a newer framework, but the location and still-developing record of supervision raise questions about independent constraints as Fayda scales.²⁰⁶ Uganda has the Data Protection and Privacy Act Cap 97 and Regulations of 2021, yet the national-ID case decided on 10 June 2025 and the January 2026 connectivity restriction show that legal protection varies markedly by right and institution.²⁰⁷

In West Africa, Ghana, Nigeria and Senegal have distinct regulatory directions. Ghana's Data Protection Act, 2012 (Act 843) is older but operates alongside active judicial protection, as Gorni demonstrated in February 2026, and the 2026 L.I. 2523 rules have tightened identity-verification practice.²⁰⁸ Nigeria's Nigeria Data Protection Act, 2023 created a stronger enforcement architec-

199 Strengthening Fayda Ethiopia's improvement journey through the Digital ID Assessment <https://dial.global/wp-content/uploads/2026/05/FINAL-Ethiopia-Digital-ID-Assessment-2.pdf>

200 Digital Coloniser? China and Artificial Intelligence in Africa <https://repository.up.ac.za/server/api/core/bitstreams/7bb46df0-a858-40ad-81b3-5c76dac-82ca6/content>

201 National Identification and Registration Authority, Uganda. (2025, May 15). Press statement on the mass enrolment exercise. <https://www.nira.go.ug/publications/press-statement-on-the-mass-enrolment-exercise>

202 World Bank. (2021). Digital economy for Zimbabwe: Country diagnostic report. <https://documents1.worldbank.org/curated/en/982981621880260112/pdf/Digital-Economy-for-Zimbabwe-Country-Diagnostic-Report.pdf>; United Nations in Zimbabwe. (2026, March 14). Zimbabwe unveils 2026–2030 AI strategy to advance inclusive digital transformation. <https://zimbabwe.un.org/en/311859-zimbabwe-unveils-2026%E2%80%932030-ai-strategy-advance-inclusive-digital-transformation>; Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. <https://zimtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE-2026-National-Budget-25-November-2025-final.pdf>

203 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>; International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; International Foundation for Electoral Systems. (2023). Cybersecurity programming guide for electoral assistance. <https://www.ifes.org/sites/default/files/2023-06/Cybersecurity-Programming-Guide-USAID.pdf>

204 Personal Data Protection Center, Egypt. (2026). Legal framework: Personal Data Protection Law No. 151 of 2020 and Executive Regulations No. 816 of 2025. <https://www.pdpc.gov.eg/>; Shand Partners. (2026, January 11). Executive regulations of the data protection law in Egypt (Law No. 151 of 2020). <https://www.shand-partners.com/insights/briefings/telecoms-media-technology/the-issuance-of-the-executive-regulations-of-the-data-protection-law-and-the-establishment-of-the-data-protection-centre/>

205 Ministry of Communication Technologies, Tunisia. (n.d.). e-Houwiya / Mobile ID. Retrieved September 13, 2026, from <https://www.mobile-id.tn/accueil>

206 Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethiotelecom.et/2025-26-budget-year-annual-business-performance-report/5/>; Ministry of Justice, Ethiopia. (2024, July 24). Personal Data Protection Proclamation No. 1321/2024. <https://justice.gov.et/en/law/personal-data-protection-proclamation/>; Fayda National ID, Ethiopia. (n.d.). Fayda ID strategy. Retrieved September 13, 2026, from <https://id.gov.et/strategies>

207 Uganda Legal Information Institute. (2019). Data Protection and Privacy Act, 2019. <https://ulii.org/en/akn/ug/act/2019/9/eng@2019-05-03>; Constitutional Court of Uganda. (2026, March 17). Alternative Digitalk Limited and others v. Attorney General (Consolidated Constitutional Petitions No. 34, 37 & 42 of 2022) [2026] UGCC 3. Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/judgement/ugcc/2026/3/eng@2026-03-17>; Uganda Communications Commission. (2026, January 14). Temporary suspension of public internet access and selected mobile services. <https://www.ucc.co.ug/wp-content/uploads/2026/01/Temporary-suspension-of-public-internet-access-and-mobile-services.pdf>; Uganda Communications Commission. (2026, January 18). Public update: Restoration of public internet access. <https://www.ucc.co.ug/public-update-18th-january-2026-press-briefing-to-update-the-country/>

208 Supreme Court of Ghana. (2026, February 25). Gorni v. Vodafone Ghana Ltd and others (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification

ture, and the National Identity Management Commission Act, 2026 modernised the identity framework. The settlement of the NDPC's 2025 Meta order nevertheless illustrates that a final accountability outcome can be less stringent and less transparent than an initial enforcement announcement.²⁰⁹ Senegal's Law No. 2008-12 of 25 January 2008 remains dated, but the ECOWAS Court offers an external judicial route that proved effective against the 2023 shutdowns.²¹⁰

Southern Africa ranges from comparatively strong institutional separation to more conflicted or fragmented arrangements. South Africa's Protection of Personal Information Act 4 of 2013, which became fully effective from 1 July 2021, and the independent Information Regulator provide a stronger baseline, supplemented by the 16 January 2024 P.P.M judgement on administrative justice.²¹¹ In Zambia, the Data Protection Act operates alongside the Cyber Security Act No. 3 of 2025²¹² which established a Central Monitoring and Coordination Centre that sits under the presidency and channels communications interception through executive intelligence control, and emergency interception allowed without judicial warrants.²¹³ While the Data Protection Act and Electronic Government Act No. 41 of 2021 provide formal safeguards for data processing and electronic government, lawful interception under the Cyber Security Act heightens the need for clear checks between data-protection and security institutions.²¹⁴ Zimbabwe's Cyber and Data Protection Act, 2021 gives POTRAZ a dual telecommunications and data-protection role, creating a structural independence concern even where formal rights exist.²¹⁵

Across Africa, the election-technology record adds four urgent governance gaps. Inadequate manual/offline fallback, opaque data-sharing between EMBs and identity agencies, weak public auditability of proprietary systems, and procurement contracts that do not clearly allocate data, logs, source code, or continuity rights.²¹⁶ A further design issue is purpose limitation. However, these are governance problems first before they are technology problems.

The comparative finding is therefore not that African countries lack legal safeguards, but that enforcement maturity, institutional independence, transparency and the capacity to constrain high-impact public systems remain uneven. Stronger rights protection is evident where laws are operationalised, courts and regulators exercise independent oversight, decisions are transparent and remedies are implemented. Risks increase where the state's capacity to link, query or intercept data expands faster than the institutions and mechanisms to scrutinise and constrain that power.

4.3 Stakeholder Responsibilities on Human Rights across DPI Ecosystems

Responsibility is increasingly distributed across public agencies, regulators, banks, telecom operators, payment companies, vendors and development partners, while accountability is still organised mainly by sector. This mismatch is most visible when one

mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory-for-ghana-card-verification-under-new-li-2523/>; Ghana Legal Information Institute / Data Protection Commission. (2012, May 10). Data Protection Act, 2012 (Act 843). <https://ghalii.org/akn/gh/act/2012/843/eng@2012-05-18>

209 Premium Times. (2026, April 26). Inside Nigeria's settlement of the NDPC's US\$32.8 million Meta remedial fee. <https://www.premiumtimesng.com/news/headlines/873350-exclusive-inside-nigerias-deal-to-write-off-32-8-million-fine-against-meta.html>; State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026-into-law-as-minister-reveals-the-arrest-of-terrorists-with-nimc-database/>; Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act, 2023. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf

210 Community Court of Justice, ECOWAS. (2025, May 14). L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JUD-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-L'INFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>; Commission de Protection des Données Personnelles, Senegal. (2008). Law No. 2008-12 of 25 January 2008 on the protection of personal data. <https://www.cdp.sn/legislation/textes-legislatifs>

211 High Court of South Africa, Gauteng Division. (2024, January 16). P.P.M. and others v. Minister of Home Affairs and others (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>; Information Regulator of South Africa. (2026). Annual performance plan 2026/27. <https://infoeregulator.org.za/strategic-reports/>; Government of South Africa. (2013). Protection of Personal Information Act 4 of 2013 (POPIA). <https://www.gov.za/documents/protection-personal-information-act>

212 National Assembly of Zambia. (2021). The Data Protection Act, 2021. <https://www.parliament.gov.zm/node/8853>; National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>

213 Zambia's new cyber laws spark fears of surveillance <https://ifex.org/zambias-new-cyber-laws-spark-fears-of-surveillance/>

214 National Assembly of Zambia. (2021). The Data Protection Act, 2021. <https://www.parliament.gov.zm/node/8853>; National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>; National Assembly of Zambia. (2021). Electronic Government Act, No. 41 of 2021. <https://www.parliament.gov.zm/node/9014>

215 Zimbabwe Legal Information Institute. (2022, March 11). Cyber and Data Protection Act, 2021 (Chapter 12:07). <https://zimlii.org/akn/zw/act/2021/5/eng@2022-03-11>

216 International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; International Foundation for Electoral Systems. (2023). Cybersecurity programming guide for electoral assistance. <https://www.ifes.org/sites/default/files/2023-06/Cybersecurity-Programming-Guide-USAID.pdf>

failure crosses identity, communications, payments, and public services.

4.3.1 Roles of Private Companies, Donors, and Technology Providers

The design, implementation, and daily operation of African DPI ecosystems are co-produced across a mix of state, market, and non-state actors, rather than governments alone. State identity agencies and interior ministries hold formal legal custody over, and are responsible for civic registration, ID issuance, and national population registers. The operational authority is shared with central banks, tax authorities and ICT ministries. Development partners, telecom operators, banks, biometric vendors, payment-switch operators and systems integrators perform material financing, enrollment, authentication or service-delivery roles. These operational functions determine whether citizens can enrol, authenticate, pay, or access a public service.

Commercial telecom operators, banks and private vendors have become the indispensable operational arms of state DPI. In Ethiopia, Ethio Telecom reported in August 2026 that it had registered nearly 32 million people for Fayda while also operating connectivity and Telebirr.²¹⁷ South African banks provide Smart ID services under the Department of Home Affairs' partnership model.²¹⁸ In Ghana, NIA, NITA, Ghipss, financial institutions and technology contractors such as Margins Group and IMS hold distinct parts of the identity, data and payment stack.²¹⁹ In Nigeria, the identity-payment environment depends on NIMC and NIBSS alongside banks and telecom operators.²²⁰ Development finance supports major programmes in Ethiopia, Nigeria, Senegal and Zambia.²²¹ In Kenya, a consortium led by Webmasters Limited has operated the eCitizen portal since 2014, IDEMIA provided Huduma Namba devices,²²² Safaricom operates M-PESA, while Smartmatic has provided election technology. Public authorities nevertheless retain the duty to protect rights and cannot outsource accountability with the technology. In Zimbabwe, Econet Wireless operates EcoCash where it has 73.75% market share.²²³ In Tunisia, Uqodo provides AI biometric verification for e-Hou-wiya.²²⁴

International financial institutions fund and shape national DPI architecture through concessional loans, technical assistance, and disbursement milestones. For example, the World Bank (ID4D and IDA) underwrites the development of foundational DPI projects in Ethiopia, Nigeria, Ghana, Zambia, Senegal, Tunisia and Egypt. Donor co-financing is also evident in the partnership between the World Bank, AFD and EIB in Nigeria. In addition, philanthropic organisations such as Gates Foundation,²²⁵ UNDP,²²⁶ Co-Develop, and the 50-in-5 campaign promotes open standards and rapid deployment. FinMark Trust and Co-Develop are building a regional DPI which includes a federated electronic Know Your Customer (eKYC) ecosystem spanning 16 member states in support of the Southern Africa Development Community (SADC) payment systems.²²⁷ The open-source (Modular Open Source

217 Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethiotelcom.et/2025-26-budget-year-annual-business-performance-report/5/>

218 SAnews. (2026, June 24). More than 200 bank branches now offering Smart ID card. <https://www.sanews.gov.za/south-africa/more-200-bank-branches-now-offering-smart-id-card>

219 National Information Technology Agency, Ghana. (2025). Data Harmonisation Bill: Proposed National Data Exchange Platform and interoperability framework. <https://nita.gov.gh/wp-content/uploads/2025/NITA-Data-Harmonisation-Bill.pdf>; Ghana Interbank Payment and Settlement Systems. (2026). Industry performance: 2025 transaction volume and value. <https://ghipss.net/component/content/category/56-newsletters>; National Identification Authority, Ghana. (2026, March 27). Government makes biometric verification mandatory for Ghana Card verification under new L.I. 2523. <https://nia.gov.gh/government-makes-biometric-verification-mandatory-for-ghana-card-verification-under-new-l-i-2523/>

220 Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry–NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>; State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026-into-law-as-minister-reveals-the-arrest-of-terrorists-with-nimc-database/>; Nigeria Inter-Bank Settlement System. (2025, June 23). NIBSS unveils the National Payment Stack to power the future of instant payments in Nigeria. <https://nibss-plc.com.ng/nibss-unveils-the-national-payment-stack-to-power-the-future-of-instant-payments-in-nigeria/>

221 World Bank. (2026, January 28). Senegal Digital Economy Acceleration Project: Restructuring paper. <https://documents1.worldbank.org/curated/en/099013026050538641/pdf/P172524-9a862e0b-dfb7-46ab-8c90-3096cadd5e1a.pdf>; Fayda National ID, Ethiopia (accessed 13 September 2026). Official programme overview — foundational digital ID under Proclamation No. 1284/2023. <https://www.id.gov.et/>; World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>; Nigeria Inter-Bank Settlement System. (2025, June 23). NIBSS unveils the National Payment Stack to power the future of instant payments in Nigeria. <https://nibss-plc.com.ng/nibss-unveils-the-national-payment-stack-to-power-the-future-of-instant-payments-in-nigeria/>

222 The East African. (2019, July 6). Kenyan MPs vote to block French firm Idemia from the country <https://www.theeastafrican.co.ke/tea/news/east-africa/kenyan-mps-vote-to-block-french-firm-idemia-from-the-country-1416630>; The Elephant. (2022, August 3). Smartmatic: The Election Company and their Role in the Upcoming Elections <https://www.theelephant.info/analysis/2022/08/03/smartmatic-the-election-company-and-their-role-in-the-upcoming-elections/>

223 Econet Wireless Zimbabwe – Integrated Annual Report 2026 <https://ewzinvestor.com/econet-wireless-zimbabwe-integrated-annual-report-2026/>

224 Tunisia drives digitization agenda forward while navigating risks <https://www.biometricupdate.com/202503/tunisia-drives-digitization-agenda-forward-while-navigating-risks>

225 Digital IDs are an effective tool against poverty <https://www.gatesfoundation.org/ideas/articles/mosip-digital-id-systems>

226 Digital Public Infrastructure <https://www.undp.org/digital/digital-public-infrastructure>

227 Strategic Collaboration Establishes Africa's First Cross-Border Digital Identity Framework, Enabling Financial Inclusion for Millions <https://www.codevelop>

Identity Platform (MOSIP), funded by the Bill & Melinda Gates Foundation, Omidyar Network and Tata Trusts, has been adopted as an affordable interoperable core foundational software in Ethiopia, Uganda and Zambia to prevent proprietary vendor lock-in.²²⁸ Smart Africa is spearheading continental efforts to harmonize digital identity and build resilient Digital Public Infrastructure (DPI) across its member states.²²⁹

Civil society organizations (CSOs) are almost universally excluded from upfront system design, forced to rely on strategic litigation as a reactive check against executive overreach. In Kenya, litigation by Katiba Institute, Haki Na Sheria and Nubian Rights Forum prompted the High Court to halt the implementation of Huduma Namba and Maisha Namba for lacking a Data Protection Impact Assessment (DPIA).²³⁰ In South Africa, litigation by Lawyers for Human Rights (LHR) resulted in the High Court striking down the Department of Home Affairs' practice of "ID blocking" without administrative due process, finding that it constituted an unjust and irregular administrative action that was inconsistent with the Constitution.²³¹ In Ghana, *Gorni v Vodafone Ghana Ltd* resulted in a Supreme Court ruling in February 2026 declaring the unauthorized linking of SIM cards to mobile money accounts a violation of constitutional privacy.²³²

A similar case was decided in Kenya, where the High Court affirmed that mobile phone numbers form an integral part of an individual's digital identity and are protected under the constitutional right to privacy, and expressly prohibited telecommunications companies, including Safaricom, from automatically recycling inactive or dormant phone numbers without the consent of the original subscriber.²³³ Other cases have been brought by civil society such as the Initiative for Social Economic Rights (ISER), Health Equity and Policy Initiative Limited, and the Unwanted Witness in Uganda.²³⁴ Also, CIPESA, Article19 Global, and Access Now successfully joined the Digital Identity case by ISER and others as *amicus curiae*.²³⁵ Other cases have been brought by civil society such as SERAP and Paradigm Initiative in Nigeria,²³⁶ MISA Zimbabwe and Zimrights in Zimbabwe,²³⁷ and AfricTivistes and Media Defence in Senegal.²³⁸

Across Africa, election-management bodies have also become central players in the DPI. As national identity and population data become inputs to voter registration, EMBs, while constitutionally remaining responsible for managing the electoral process, depend on identity agencies, telecom operators, data centres, biometric suppliers and systems integrators for routine voter registration and verification.²³⁹ Election technology systems widens the circle of private responsibility to include biometric-kit suppliers, hosting and cloud providers, cybersecurity firms, telecom networks and results-platform integrators. Their products can be directly linked to political participation, privacy and public trust even where the election authority remains the primary duty-bearer.²⁴⁰

[fund/insights-1/strategic-collaboration-establishes-africas-first-cross-border-digital-identity-framework-enabling-financial-inclusion-for-millions](#)

228 Why countries need an open and affordable identity solution <https://www.id4africa.com/2019/almanac/MOSIP.pdf>

229 Digital Public Infrastructure: Africa's Hidden Engine for Inclusion and transformation <https://dpi.africa.com/digital-public-infrastructure-africas-hidden-engine-for-inclusion-and-transformation/>

230 Kenyan high court pauses national digital ID for third time in 4 years <https://www.biometricupdate.com/202407/kenyan-high-court-pauses-national-digital-id-for-third-time-in-4-years>

231 PRESS STATEMENT | Home Affairs practice of "ID blocking" declared unconstitutional <https://www.lhr.org.za/lhr-news/press-statement-home-affairs-practice-of-id-blocking-declared-unconstitutional/>

232 ELORM KWAMI GORNI V. VODAFONE GHANA LIMITED & ORS <https://www.judy.legal/case/elorm-kwami-gorni-v-vodafone-ghana-limited-ors>

233 Kenya dispatch: High Court bars recycling of dormant phone numbers without consent <https://www.jurist.org/news/2026/03/kenya-dispatch-high-court-bars-recycling-of-dormant-phone-numbers-without-consent/#>

234 Civil Society sues Government over Ndaga Muntu National ID: Mandatory Digital ID Threatens Lives! https://www.unwantedwitness.org/download/Digital-ID-Litigation_-_PRESS-STATEMENT-FINAL.pdf

235 CIPESA, "Court Admits Expert Views from CIPESA, Access Now and Article 19 on Uganda's Digital ID," March 2023, <https://cipesa.org/2023/03/court-admits-expert-views-from-cipesa-access-now-and-article-19-on-ugandas-digital-id/>

236 Press Release: Paradigm Initiative files a public-interest case to challenge recent data breach that saw personal data sold for N100 <https://paradigmhq.org/press-release-paradigm-initiative-files-a-public-interest-case-to-challenge-recent-data-breach-that-saw-personal-data-sold-for-n100/>

237 Zimbabwe High Court Orders restoration of the Internet <https://dig.watch/updates/zimbabwe-high-court-orders-restoration-internet>

238 Activists filed a lawsuit before the ECOWAS Court of Justice to challenge Internet shutdowns in Senegal <https://www.business-humanrights.org/es/%C3%BAltimas-noticias/activistes-filed-a-lawsuit-before-the-ecowas-court-of-justice-to-challenge-internet-shutdowns-in-senegal/>

239 International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; International Foundation for Electoral Systems. (2023). Cybersecurity programming guide for electoral assistance. <https://www.ifes.org/sites/default/files/2023-06/Cybersecurity-Programming-Guide-USAID.pdf>

240 International Foundation for Electoral Systems. (2023). Cybersecurity programming guide for electoral assistance. <https://www.ifes.org/sites/default/files/2023-06/Cybersecurity-Programming-Guide-USAID.pdf>

4.3.2 Human Rights Due Diligence in DPI Design and Deployment

Publicly available, project-specific human-rights due diligence, human rights impact assessments or UNGP aligned disclosures by private biometric vendors, telecom operators, payment platforms and cloud providers remains rare across the 11 countries. The strongest documented accountability precedent remains the French vigilance litigation and settlement concerning IDEMIA's role in Kenya's earlier NIIMS programme.²⁴¹ Beyond that case, the public record reviewed for biometric vendors, telecom operators, payment firms, banks and system integrators contains very little project-specific UNGP-aligned disclosure covering exclusion, surveillance, downstream government use, remedy and disengagement. This is a cross-country transparency and governance gap, not proof that no internal due diligence occurs.

Across Africa, this disclosure gap is particularly serious in election technology because supplier performance is tested under adversarial conditions and immovable deadlines.

4.3.3 Accountability Mechanisms for Addressing Harms and Their Effectiveness

In the 11 countries sampled, there are multiple oversight and accountability mechanisms, but availability is uneven. They include financial, consumer protection and telecommunications sector regulators, data protection authorities, institutional administrative correction, judicial bodies, parliamentary oversight, media investigations and civil-society monitoring.

Recent examples show these routes can work, for example, in South Africa's 16 January 2024 ID-blocking High Court judgement,²⁴² the ECOWAS Court's 14 May 2025 *ASUTIC and Ndiaga Gueye v Republic of Senegal* judgement,²⁴³ Ghana's 25 February 2026 privacy judgement, Kenya's Huduma Namba judgement that required DPIA,²⁴⁴ and Uganda's 17 March 2026 Constitutional Court decision, all imposed legal consequences on digital or DPI-adjacent practices.

Donor safeguards and project grievance mechanisms can supplement these routes, but they do not replace domestic institutions with authority over public bodies. Across Africa, courts and regional bodies are increasingly acting as design institutions when legislatures or procurement systems have not specified sufficient safeguards. Kenya's identity jurisprudence and the ECOWAS Court's 14 May 2025 Senegal shutdown judgment show how litigation can set rules on assessment, legality, and state restraint that later shape infrastructure governance more broadly.

Notably, because DPI integrates identity, telecommunications, payments, and public services, the technical integration can create an accountability diffusion gap. Typically, this means that when an individual experiences a DPI service failure at any of the three pillars, such as biometric read failure for KYC purpose to access an essential service e.g. health or finance, the failure can be attributed to the identity agency, the telecom operator, or the payment operator. As a result, the public or private actors often routinely shift blame to one another thus no single institution assumes responsibility or provides remedy. In Nigeria, following NIMC's 2025 migration of telecom operators to the NINAuth verification platform, NIMC directed citizens experiencing NIN-SIM linkage errors to mobile network operators, while MNOs referred subscribers back to NIMC centres, leaving users trapped in an administrative loop without line restoration.²⁴⁵ In Ghana, mandatory Ghana Card SIM re-registration involved overlapping mandates among the National Identification Authority (NIA), National Communications Authority (NCA), and mobile operators, with no unified inter-agency grievance protocol for citizens disconnected in error.²⁴⁶

²⁴¹ Kenya Human Rights Commission. (2023, November). NGOs and IDEMIA agree to vigilance plan improvements in settlement over Kenyan digital ID human rights challenge. <https://khrc.or.ke/press-release/ngos-and-idemia-agree-to-vigilance-plan-improvements-in-settlement-over-kenyan-digital-id-human-rights-challenge/>; Kenya Human Rights Commission. (2022, July 29). KHRC, Nubian Rights Forum and NGO Data Rights file case against IDEMIA in France for failure to consider human rights risks. <https://khrc.or.ke/press-release/kenya-human-rights-commission-nubian-rights-forum-and-ngo-data-rights-files-case-against-biometric-tech-giant-idemia-in-france-for-failure-to-consider-human-rights-risks/>

²⁴² High Court of South Africa, Gauteng Division. (2024, January 16). P.P.M. and others v. Minister of Home Affairs and others (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>

²⁴³ Community Court of Justice, ECOWAS. (2025, May 14). L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JUD-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-LINFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>

²⁴⁴ High Court of Kenya. (2020, January 30). Nubian Rights Forum & 2 others v. Attorney General & 6 others; Child Welfare Society & 8 others (Interested Parties) (Petition 56, 58 & 59 of 2019, Consolidated) [2020] KEHC 8772 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2020/8772>

²⁴⁵ Telcos now on upgraded NIN verification platform – NIMC <https://punchng.com/telcos-now-on-upgraded-nin-verification-platform-nimc/>; Direct all NIN-SIM issues to telecom operators, NIMC tells Nigerians as it completes migration to NINAuth <https://nairametrics.com/2025/07/30/direct-all-nin-sim-issues-to-telecom-operators-nimc-tells-nigerians-as-it-completes-migration-to-ninauth/>

²⁴⁶ Ghana disconnects unregistered SIMs <https://www.connectingafrica.com/regulation/ghana-disconnects-unregistered-sims>; IMANI Alert: SIM Card Re-registration Exercise – A Decade and a Half of Policy Failure <https://imaniafrica.org/2026/03/imani-alert-sim-card-re-registration-exercise-a-decade-and-a-half-of-policy-failure/>

Furthermore, sectoral regulators face acute structural conflicts. In Ethiopia and Zimbabwe, the supervisory data protection authority is embedded inside the telecommunications regulator ECA²⁴⁷ and POTRAZ²⁴⁸ respectively. In Uganda, the Personal Data Protection Office (PDPO) sits organizationally inside NITA-U, the agency tasked with driving state digital transformation in the country and also operates the UGHub and the government cloud.²⁴⁹

4.3.4 Accessibility of Grievance and Remedy Mechanisms for Affected Populations

While formal complaint channels exist on paper across most study countries, their practical accessibility for vulnerable and marginalized populations remains severely constrained by procedural, financial, geographic, and digital-literacy barriers.²⁵⁰ In the context of DPI, the most important test is whether a person can identify one responsible body, correct an identity record, challenge unauthorised processing, obtain an explanation for a decision, and restore access to essential services within a meaningful timeframe before a linked failure spreads to other services.

Digital-first complaint mechanisms operated by DPAs, such as South Africa's Information Regulator's eServices portal,²⁵¹ Senegal's CDP online form,²⁵² Kenya's ODPC complaints form,²⁵³ Nigeria's NDPC portal,²⁵⁴ are useful. However, access requires internet connectivity, formal written submissions, and digital literacy, which could also create a barrier for traditionally digitally excluded communities, incapable of navigating online complaint portals. Also, the physical remedy routes to the state and non-state bodies operating the DPI systems have weak remedy mechanisms, often resulting in aggrieved parties resorting to courts for remedies.

South Africa's P.P.M case shows that courts can correct unlawful ID blocking, but it also arose after prolonged administrative difficulty.²⁵⁵ In Uganda, the 2025 national-ID exclusion dispute reached the High Court through public-interest litigation, illustrating the distance between formal complaint pathways and judicial remedy for systemic claims.²⁵⁶ Zambia divides responsibility among the Data Protection Commissioner, telecom and cybersecurity institutions, and service agencies,²⁵⁷ while Zimbabwe divides identity, telecommunications/data protection. and payment oversight among separate bodies.²⁵⁸

Remedy mechanisms often remain inaccessible to vulnerable groups such as refugees, indigenous communities and undocumented citizens. In Ethiopia, World Bank results reporting in September 2025 showed refugee host-community Fayda enrolments sitting at zero against a 1.7 million target, while displaced populations in conflict zones (Tigray, Amhara) have no physical or administrative access to ECA grievance channels.²⁵⁹ In Kenya, Nubians and Somali-Kenyans historically faced discriminatory vetting committees, yet new changes abolishing the committees have introduced due process concerns without a specialized administrative appeal body.²⁶⁰ In Uganda, the indigenous Benet community remains unrepresented in NIRA registries, locking

247 Ethiopia's Personal Data Protection Proclamation of 2024 and its Budding Digital Identity Regime <https://cipit.strathmore.edu/ethiopias-personal-data-protection-proclamation-of-2024-and-its-budding-digital-identity-regime/>

248 Data Protection Act <https://www.potraz.gov.zw/wp-content/uploads/2022/02/Data-Protection-Act-5-of-2021.pdf>

249 Personal Data Protection Office <https://www.nita.go.ug/services/personal-data-protection-office>; Integration Service (UGHub) <https://www.nita.go.ug/services/e-government-services/integration-service-ughub>

250 Sesan, 'G. and Roberts, T. (eds) (2025) Biometric Digital-ID in Africa: Progress and Challenges to Date – Ten Country Case Studies, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2025.051 https://opendocs.ids.ac.uk/Biometric_Digital-ID_in_Africa?_gl=1*1igvytu*_gcl_au*MTIyNTcwNTM1MC4xNzkwND-k3MDE1

251 eServices <https://eservices.inforegulator.org.za/>

252 Plainte et Signalement <https://www.cdp.sn/plainte>

253 File/Lodge a complaint <https://www.odpc.go.ke/file-a-complaint/>

254 Data breach <https://services.ndpc.gov.ng/breach/>

255 High Court of South Africa, Gauteng Division. (2024, January 16). P.P.M. and others v. Minister of Home Affairs and others (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>

256 High Court of Uganda, Civil Division. (2025, June 10). Initiative for Social and Economic Rights (ISER) and 2 others v. Attorney General and another (Miscellaneous Cause No. 0086 of 2022) [2025] UGHCCD 90. <https://ulii.org/en/akn/ug/judgement/ughccd/2025/90/eng@2025-06-10>

257 National Assembly of Zambia. (2021). The Data Protection Act, 2021. <https://www.parliament.gov.zm/node/8853>; National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>

258 Zimbabwe Legal Information Institute. (2022, March 11). Cyber and Data Protection Act, 2021 (Chapter 12:07). <https://zimlil.org/akn/zw/act/2021/5/eng@2022-03-11>; Reserve Bank of Zimbabwe. (2020, July 9). Designation of ZIMSWITCH as a national payment switch. https://www.rbz.co.zw/documents/press/July/00100_-_Press-Statement---Zimswitch-Designation-as-National-Switch---9-7-2020-2.pdf

259 Ethiopia Digital ID for Inclusion and Services Project (P179040) <https://documents1.worldbank.org/curated/en/099102925060510930/pdf/P179040-49e3036e-1e1a-40ff-97e0-ef57cb36f7.pdf>

260 Kenya's vetting process against Nubians and border communities improved, but due process concerns still remain <https://www.institutesi.org/news/kenyas-vetting-process-against-nubians-and-border-communities>

them out of social safety nets without an accessible local grievance desk.²⁶¹

Across Africa, elections expose the importance of remedy speed. A complaint mechanism that answers after polling may be legally available but practically ineffective for an eligible voter. Pre-election correction deadlines, on-site exception procedures, extended voting where justified, and preservation of paper or human-readable evidence should therefore be treated as remedy architecture.²⁶²

4.3.5 Effectiveness of Remedy for Affected Populations

Evaluating UNGP Pillar 3 across all 11 study countries reveals a profound divide that strategic litigation brought by well-resourced civil society organizations has successfully secured structural remedies from courts, but ordinary citizens facing individual DPI harms almost never receive timely, individual-level remedy or financial compensation.

Effective remedy remains uncommon, but several recent decisions at regional and domestic levels show that it is possible. Some case outcomes have included structural remedies such as in South Africa, where on 16 January 2024, the Gauteng High Court in *P.P.M. and Others v Minister of Home Affairs and Others* struck down unconstitutional blocking of IDs and required procedural fairness and provided relief for the affected litigants.²⁶³ Similarly, Kenya's High Court in December 2023 halted Maisha Namba for lack of statutory DPIA.²⁶⁴ Another Kenyan remedy is significant because it concerns errors propagating between identity systems. In *Haki na Sheria Initiative & 3 others v Attorney General & 4 others*, decided by the High Court at Garissa on 21 January 2025, the court held that refusal to remove Kenyan citizens who had been vetted and cleared from the refugee database, and the resulting failure to issue identity documents, violated constitutional rights.²⁶⁵ It ordered the successful petitioners' names removed, directed issuance of identity documents within 60 days, required cleared double-registration cases to be deregistered, and ordered the responsible authorities to constitute or reactivate vetting committees for unresolved cases. The case is an example of cross-system correction and effective judicial remedy, while also illustrating how costly and slow correction can be when administrative databases conflict.

Courts have also applied retrospective remedies, including at the regional level. In February 2026, Ghana's Supreme Court held that the unauthorised linking of a SIM and mobile-money account to using an individual's Ghana Card details without their breached constitutional privacy and attracted damages.²⁶⁶ Senegal provides a binding regional remedy through the ECOWAS Court's 14 May 2025 judgment which declared shutdowns illegal and ordered damages.²⁶⁷ Uganda provides a mixed outcome, as the June 2025 national-ID exclusion challenge failed, while the 17 March 2026 Alternative Digitalk judgement strengthened expression protections.²⁶⁸ Also, Nigeria's NDPC in November 2025, reversed Meta's USD 32.8 million penalty via consent judgment.²⁶⁹ Remedy should therefore be assessed by right, institution and implementation rather than by a single country.

Across Africa, effective electoral remedy must be both institutionally independent and temporally capable of preventing irreversible harm. Regional and domestic courts can correct unlawful restrictions, but administrative systems also need lower-cost remedies that work before a polling deadline or service cut-off. The goal is not to judicialise every failure, but to make courts the

²⁶¹ Indigenous community in Uganda seeks an end to their statelessness <https://www.unhcr.org/news/stories/indigenous-community-uganda-seeks-end-their-statelessness>

²⁶² International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

²⁶³ High Court of South Africa, Gauteng Division. (2024, January 16). *P.P.M. and others v. Minister of Home Affairs and others* (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>

²⁶⁴ **Nation Africa, High Court halts Maisha Namba rollout over legal basis, DPIA and participation concerns. ** <https://nation.africa/kenya/news/high-court-puts-the-brakes-on-kindiki-s-plan-to-introduce-maisha-namba-4454474>

²⁶⁵ High Court of Kenya at Garissa. (2025, January 21). *Haki na Sheria Initiative & 3 others v. Attorney General & 4 others* (Petition E008 of 2021) [2025] KEHC 221 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2025/221/eng@2025-01-21>

²⁶⁶ Supreme Court of Ghana. (2026, February 25). *Gorni v. Vodafone Ghana Ltd and others* (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>

²⁶⁷ Kenyalaw. (2024, August 12). *Haki na Sheria Initiative v. Attorney General & 4 others* [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>; Community Court of Justice, ECOWAS. (2025, May 14). *L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal* (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JU-D-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-L'INFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>

²⁶⁸ Constitutional Court of Uganda. (2026, March 17). *Alternative Digitalk Limited and others v. Attorney General* (Consolidated Constitutional Petitions No. 34, 37 & 42 of 2022) [2026] UGCC 3. Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/judgement/ugcc/2026/3/eng@2026-03-17>; High Court of Uganda, Civil Division. (2025, June 10). *Initiative for Social and Economic Rights (ISER) and 2 others v. Attorney General and another* (Miscellaneous Cause No. 0086 of 2022) [2025] UGHCCD 90. <https://ulii.org/en/akn/ug/judgement/ughccd/2025/90/eng@2025-06-10>

²⁶⁹ Nigeria and Meta agree to settle USD 32.8 million data protection dispute <https://iclg.com/news/23143-nigeria-and-meta-agree-to-settle-usd-32-8-million-data-protection-dispute/>

backstop rather than the first or primary route to remedy breaches or violations

Responsibility becomes harder to see as DPI becomes more interconnected. In Egypt²⁷⁰ and Tunisia,²⁷¹ ministries and state agencies retain strong control over identity and public data, while telecom and technology firms provide operational services within political environments where independent public scrutiny is constrained. Ethiopia adds a distinctive institutional development, as since 4 August 2026, Faydaverse has been a state-owned enterprise responsible for developing, operating, and scaling national DPI, while Ethio Teleco, which is also majority state-owned, is simultaneously important to connectivity, Telebirr, and Fayda enrolment.²⁷² This concentration can improve coordination, but it also makes clear rules on access, audit, institutional separation, and oversight more important.

Kenya, Ghana and Nigeria show how private intermediaries become part of public infrastructure. Safaricom and other providers sit inside Kenya's payment and authentication environment. Ghana's identity programme relies on private technical partners while telecom and mobile-money operators use Ghana Card verification; and Nigeria's banks, telecom operators, NIBSS and identity verification agents can determine whether a person is successfully recognised across several services.²⁷³ In all three cases, the state remains the primary duty-bearer, but effective accountability must also reach the companies whose systems or decisions create the point of access. However, evidence shows that most remedies are not always obtained within the company's remedy channels.

The developments around remedies appear to be strongest where several accountability routes overlap. South Africa combines the Information Regulator, courts, and active civil society.²⁷⁴ Ghana's Supreme Court created an individual privacy remedy in February 2026 alongside the Data Protection Authority.²⁷⁵ Senegalese applicants used the ECOWAS Court after the 2023 shutdowns. Also, Kenya's civil society has repeatedly used constitutional and data-protection litigation.²⁷⁶ Nigeria's regulator demonstrates that enforcement power exists, but the October–November 2025 settlement with Meta, reported in April 2026 to have removed the USD 32.8 million remedial fee while retaining compliance commitments, shows why accountability should be judged by the final outcome and disclosure of a case, not only the size of an initial sanction.²⁷⁷

Uganda, Zambia and Zimbabwe illustrate the practical consequences of fragmented routes. Uganda has courts, the PDPO, NIRA, UCC and sector regulators, yet the identity-exclusion case, the January 2026 connectivity restriction and the March 2026 free expression judgement produced very different results.²⁷⁸ Zambia distributes complaints and oversight across data-protection, telecom, cybersecurity, payment and public-service institutions.²⁷⁹ Zimbabwe has formal routes through POTRAZ, courts and sector regulators but less public evidence on cross-system complaint outcomes.²⁸⁰ The common challenge is not the total absence of institutions; it is the difficulty for an affected person to identify which institution can correct a problem before it spreads across connected services.

270 State Information Service, Egypt. (2026, July 21). Communications Minister: Egypt to offer more than 270 digital government services by end-2026. <https://sis.gov.eg/en/media-center/news/communications-minister-egypt-to-offer-more-than-270-digital-government-services-by-end-2026/>

271 Ministry of Communication Technologies, Tunisia. (n.d.). e-Houwiya / Mobile ID. Retrieved September 13, 2026, from <https://www.mobile-id.tn/accueil>

272 Fayda National ID, Ethiopia (accessed 13 September 2026). Official programme overview — foundational digital ID under Proclamation No. 1284/2023. <https://www.id.gov.et/>; Ethiopian Investment Holdings. (2026, August 4). National ID Program reestablished as state-owned enterprise “Faydaverse” to anchor nationwide digital public infrastructure. <https://eih.et/national-id-program-reestablished-as-state-owned-enterprise-faydaverse-to-anchor-nationwide-digital-public-infrastructure-and-joins-ethiopian-investment-holdings-portfolio/>

273 Federal Ministry of Information and National Orientation, Nigeria. (2026, July 8). FG intensifies nationwide digital identity enrolment through Information Ministry–NIMC partnership. <https://fmino.gov.ng/fg-intensifies-nationwide-digital-identity-enrolment-through-information-ministry-nimc-partnership/>

274 High Court of South Africa, Gauteng Division. (2024, January 16). P.P.M. and others v. Minister of Home Affairs and others (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>

275 Supreme Court of Ghana. (2026, February 25). Gorni v. Vodafone Ghana Ltd and others (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>

276 Kenyalaw. (2024, August 12). Haki na Sheria Initiative v. Attorney General & 4 others [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>

277 Premium Times. (2026, April 26). Inside Nigeria's settlement of the NDPC's US\$32.8 million Meta remedial fee. <https://www.premiumtimesng.com/news/headlines/873350-exclusive-inside-nigerias-deal-to-write-off-32-8-million-fine-against-meta.html>

278 Constitutional Court of Uganda. (2026, March 17). Alternative Digitalk Limited and others v. Attorney General (Consolidated Constitutional Petitions No. 34, 37 & 42 of 2022) [2026] UGCC 3. Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/judgement/ugcc/2026/3/eng@2026-03-17>; Uganda Communications Commission. (2026, January 14). Temporary suspension of public internet access and selected mobile services. <https://www.ucc.co.ug/wp-content/uploads/2026/01/Temporary-suspension-of-public-internet-access-and-mobile-services.pdf>; Uganda Communications Commission. (2026, January 18). Public update: Restoration of public internet access. <https://www.ucc.co.ug/public-update-18th-january-2026-press-briefing-to-update-the-country/>

279 World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>

280 World Bank. (2021). Digital economy for Zimbabwe: Country diagnostic report. <https://documents1.worldbank.org/curated/en/982981621880260112/pdf/Digital-Economy-for-Zimbabwe-Country-Diagnostic-Report.pdf>

In all 11 countries, private-sector human-rights due diligence remains the least visible accountability layer. Public evidence of project-specific UNGP-aligned assessments by biometric vendors, telecom companies, payment operators or system integrators is scarce. This does not establish that internal processes are absent; it shows that citizens, regulators and researchers often cannot verify what risks were identified, how downstream government use was considered, or what remedy a company will provide.

The strongest accountability environments are those with more than one credible route to challenge: independent regulators, courts, civil society and sector regulators. South Africa and Kenya are comparatively strongest on this dimension. Nigeria and Ghana show growing institutional capacity; Senegal's regional remedy is important. Ethiopia, Uganda and Egypt face the most pronounced structural accountability risks, while Zambia, Zimbabwe and Tunisia illustrate how fragmented or under-developed remedy can persist even where formal institutions exist.

4.5 Rights-Respecting, Inclusive, Accountable DPI Governance

Rights-respecting DPI is most likely to be achieved where safeguards are built into design and backed by institutions that can act independently before and after harm. The evidence from the study countries demonstrates that legal or judicial progress can coexist with continuing implementation failures, so enabling conditions must be sustained rather than be treated as one-off compliance steps.

Election technology and DPI also offer reciprocal lessons. Those designing and governing DPI can learn from election systems on contestability, human-readable evidence, observation, fixed-deadline correction, incident disclosure and tested offline continuity.²⁸¹ Conversely, those designing and governing election management technology can draw on DPI principles to apply data minimisation, purpose limitation, selective interoperability, privacy and security by design, reusable open standards and lifecycle impact assessment.²⁸² The common principle is that shared infrastructure should reduce duplication without collapsing independent mandates or eliminating the evidence needed to challenge a decision.

4.5.1 Reform Priorities

Achieving rights-respecting DPI across Africa requires shifting from the conventional “DPI readiness” metrics, which measure success by enrolment volume, portal launches, and transaction speed, toward a model that incorporates democracy and human rights. Under this approach, rights protection, rule of law, user agency, and multi-stakeholder participation are treated as foundational infrastructure requirements rather than optional additions made after systems have been scaled up. The most urgent gaps are exclusive digital or biometric gateways, slow correction of foundational records, weak publication of impact assessments and audit results, opaque cross-agency access, purpose limitation, and insufficient safeguards for connectivity during elections. The general priorities include preserving assisted and non-digital access where necessary, creating clear correction routes that propagate across linked systems, require DPIA/HRIA before material expansion, and ensuring national-security access is lawful, necessary, proportionate, and subject to independent oversight and review; and ratification of the Malabo Convention.

Several countries are adopting more modular or federated approaches and expanding alternative channels. Federated exchange in Tunisia²⁸³ and South Africa²⁸⁴ can reduce unnecessary centralisation, while open-source architectures such as MOSIP adopted by Ethiopia are cost-effective and can reduce some forms of vendor lock-in.²⁸⁵ However, neither design choice is a substitute for logging, role-based access, security testing, auditability, clear retention limits, and enforceable rules on secondary use. The remaining challenge is that information in the public domain is still thin on whether these systems are audited for rights impacts after launch and whether citizens can see who accessed their data and why.

281 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>; International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; African Commission on Human and Peoples' Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achprres655lxxvi-2026>; International Foundation for Electoral Systems. (2023). Cybersecurity programming guide for electoral assistance. <https://www.ifes.org/sites/default/files/2023-06/Cybersecurity-Programming-Guide-USAID.pdf>

282 African Union Commission. (2023, December 11). AU interoperability framework for digital ID. https://www.au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf

283 Ministry of Communication Technologies, Tunisia. (n.d.). e-Houwiya / Mobile ID. Retrieved September 13, 2026, from <https://www.mobile-id.tn/accueil>

284 MyMzansi / Government of South Africa. (n.d.). Functional digital identity (Initiative 1). <https://www.mymzansi.gov.za/roadmap/initiative-1>; National Treasury, South Africa. (2025, October 9). MzansiXchange pilot launch. <https://mzansixchange.treasury.gov.za/pilot/>

285 Fayda National ID, Ethiopia (accessed 13 September 2026). Official programme overview — foundational digital ID under Proclamation No. 1284/2023. <https://www.id.gov.et/>; MOSIP. (n.d.). The MOSIP Project https://www.mosip.io/mosip_project

There are also country-specific reforms that can ensure alignment with international human rights standards. Egypt is in the first year of operationalising its 2020 data-protection law while expanding Digital Egypt and the Haweya financial-identity platform.²⁸⁶ It should structurally insulate the Personal Data Protection Center (PDPC) from executive control; narrow the broad Article 7 national security and Central Bank exemptions under Law 151/2020; repeal or reform Article 79 interception powers under the 2018 Cybercrime Law; and enact a dedicated Digital ID law establishing explicit purpose limitation, data minimization, and non-digital service fallbacks prior to the launch of the Haweya Digital Financial Identity platform and online-only Digital Egypt. Ethiopia's move to Faydaverse creates an opportunity to clarify independence, commercial incentives, and public accountability before the new institutional model hardens.²⁸⁷ It should aim to separate data protection supervision from the telecommunications regulator (ECA) into an independent, legally insulated commission; address enrollment access gaps for marginalised groups before mandatory Fayda links to banking and public services; publish disaggregated enrolment and authentication failure statistics; and establish statutory purpose limitations and access-log auditing for Fayda.

Ghana should enact the Data Protection Bill 2025 to secure the independence of the Data Protection Commission (DPC) and enforce ex ante Data Protection Impact Assessments (DPIAs); mandate full transparency and accountability of the 2018 Margins Group / IMS Public-Private Partnership (PPP) contract. Kenya should mandate published, pre- and post-deployment DPIAs for the digital identity or e-service platforms in line with court precedents; abolish discriminatory vetting processes for border and minority communities; strengthen oversight of state data sharing; and publish independent technical and financial audits of existing government e-service platforms such as eCitizen and SHA.

Nigeria has a stronger statutory data-protection framework than it did before 2023 and a modernised identity law from June 2026, but the Meta settlement demonstrates that enforcement outcomes can change even after a regulatory sanction.²⁸⁸ It should subject public-sector identity controllers such as NIMC to the same NDPC administrative fines as commercial entities; conduct an independent forensic audit of NIMC's identity-verification licensing and API access regime following the 2024 commercial data leaks that exposed up to 43 million citizens' records; establish rules on data protection enforcement to ensure transparency of regulatory rollbacks; and close the persistent gender enrolment gap. Senegal should review and reform the outdated data protection law Act No. 2008-12 to enhance safeguards; institutionalise the ECOWAS Court of Justice judgment against arbitrary state shutdowns; adequately resource the Commission de Protection des Données Personnelles (CDP) to enable cross-sector enforcement; and formalize structured civil-society participation in DPI roll-out.

South Africa should finalize and enact the National Identification and Registration Bill ahead of the 2027/2028 operational roll-out of the MyMzansi Digital ID ecosystem; guarantee unconditional birth registration pathways for undocumented, stateless, and abandoned children; formalizing permanent, constitutionally sound surveillance oversight; and mandate the publication of ex-ante Data Protection Impact Assessments (DPIAs) within MzansiXchange federated data layer. Tunisia should accelerate the adoption of the Organic Data Protection Reform Bill (PLO 095/2025) that elevates the INPDP to an independent enforcement authority before Mobile ID becomes mandatory; narrow or repeal the repressive provisions of Decree-Law 2022-54 that criminalize free speech and mandate broad digital surveillance; establish privacy safeguards and mandatory DPIA around the Mobile ID (e-Houwiya) and the Unique Citizen Identifier (IUC); and reserve non-digital administrative pathways for the digital-only service entry points.²⁸⁹

Uganda's March 2026 Constitutional Court judgement strengthened the protection of freedom of expression, while identity-re-

286 State Information Service, Egypt. (2026, July 21). Communications Minister: Egypt to offer more than 270 digital government services by end-2026. <https://sis.gov.eg/en/media-center/news/communications-minister-egypt-to-offer-more-than-270-digital-government-services-by-end-2026/>; Personal Data Protection Center, Egypt. (2026). Legal framework: Personal Data Protection Law No. 151 of 2020 and Executive Regulations No. 816 of 2025. <https://www.pdpc.gov.eg/>; Shand Partners. (2026, January 11). Executive regulations of the data protection law in Egypt (Law No. 151 of 2020). <https://www.shandpartners.com/insights/briefings/telecoms-media-technology/the-issuance-of-the-executive-regulations-of-the-data-protection-law-and-the-establishment-of-the-data-protection-centre/>; Central Bank of Egypt. (2025, November 16). PAFIX 2025: Digital Financial Identity platform (Haweya). <https://www.cbe.org.eg/en/news-publications/news/2025/11/16/18/47/pafix-2025>

287 Ethiopian Investment Holdings. (2026, August 4). National ID Program reestablished as state-owned enterprise "Faydaverse" to anchor nationwide digital public infrastructure. <https://eih.et/national-id-program-reestablished-as-state-owned-enterprise-faydaverse-to-anchor-nationwide-digital-public-infrastructure-and-joins-ethiopian-investment-holdings-portfolio/>; Ethio Telecom. (2026, July 24). 2025/26 budget year annual business performance report. <https://www.ethio-telecom.et/2025-26-budget-year-annual-business-performance-report/5/>

288 Premium Times. (2026, April 26). Inside Nigeria's settlement of the NDPC's US\$32.8 million Meta remedial fee. <https://www.premiumtimesng.com/news/headlines/873350-exclusive-inside-nigerias-deal-to-write-off-32-8-million-fine-against-meta.html>; State House, Nigeria. (2026, June 26). President Tinubu signs NIMC Act 2026 into law. <https://statehouse.gov.ng/president-tinubu-signs-nimc-act-2026-into-law-as-minister-reveals-the-arrest-of-terrorists-with-nimc-database/>; Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act, 2023. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf

289 Ministry of Communication Technologies, Tunisia. (n.d.). e-Houwiya / Mobile ID. Retrieved September 13, 2026, from <https://www.mobile-id.tn/accueil>; Tunis Afrique Presse / Tunisian Investment Authority. (2026, June 24). "Mobile ID" mandatory for project declarations from 1 July 2026. <https://www.tap.info.tn/en/Portal-Economy/20326511-mobile-id>; Tunisia Legal Database / DCAF. (2024, March 11). Organic Law No. 2024-22 amending Law No. 93-27 on the National Identity Card. <https://legislation-securite.tn/latest-laws/loi-organique-n-2024-22-du-11-mars-2024-modifiant-et-completant-la-loi-n-93-27-du-22-mars-1993-relative-a-la-carte-nationale-didentite/>; Tunisia Legal Database / DCAF. (2020, May 12). Decree-Law No. 2020-17 on the Unique Citizen Identifier. <https://legislation-securite.tn/latest-laws/decret-loi-du-chef-du-gouvernement-n-2020-17-du-12-mai-2020-relatif-a-lidentifiant-unique-du-citoyen/>

lated exclusion and election-period internet control remain unresolved patterns.²⁹⁰ This shows that a progressive reform in one area does not resolve all the challenges or remove the need for further scrutiny in other parts of the digital-governance system. Uganda should structurally decouple the PDPO from NITA-U to ensure independent regulatory oversight over NITA-U; enact statutory judicial pre-authorization requirements for all UCC internet intervention and shutdown directives to check executive overreach; enhance robust regulatory and judicial oversight over surveillance-specific technologies; and address inclusion gaps in the *Ndaga Muntu* national ID including offering alternative fallback pathways for vulnerable populations.

Zambia's World Bank-supported digital-access programme places explicit emphasis on inclusion, and the country maintained open connectivity during the August 2026 election.²⁹¹ Yet, its 2025 cybersecurity legislation raises separate interception and oversight concerns.²⁹² Therefore it should clarify the jurisdiction of the Data Protection Commission's (DPC) over cybersecurity operations and intelligence data processing; establishing strict, non-waivable judicial pre-authorization requirements for interceptions through the Central Monitoring and Coordination Centre (CMCC); mandate the proactive, public disclosure of all DPC enforcement decisions, audits and statistics of breach notifications, and administrative fines; and accelerate the deployment of the INRIS while legally preserving status of legacy paper National Registration Cards (NRCs).

Zimbabwe should structurally separate its DPA from POTRAZ to resolve the institutional conflict of interest; mandate the proactive, public disclosure of all DPA investigation statistics, enforcement outcomes, and data compliance decisions; codify strict, independent judicial warrant requirements for law enforcement access to telecom metadata; mandate ex-ante DPIA and HRIA for cross-border biometric data transfers tied to state deployments and build rights safeguards into Project Pangolin and the wider 2026–2030 AI strategy before a new national data layer reaches scale.²⁹³

4.5.2 Enabling Conditions for Rights-Respecting DPI systems

Across the comparative sample, enabling conditions do not operate in isolation. The strongest enabling conditions where rights-respecting outcomes have been achieved, have been as a result of the interaction of four mutually reinforcing dimensions, at institutional, legal, technical and civic levels.

The institutional enablers are genuinely independent oversight through adequately resourced and capable judiciaries, regulators and data protection authorities that are transparent and accountable and have statutory insulation from executive direction. South Africa's Information Regulator, Kenya's ODPC, and Nigeria's NDPC demonstrate the value of independent supervisory bodies capable of issuing binding determinations and fining public and private entities. Moreover, decisions from South Africa,²⁹⁴ Kenya,²⁹⁵ Ghana,²⁹⁶ Senegal²⁹⁷ and Uganda²⁹⁸ provide different examples of regulatory enforcement, domestic litigation, and regional adjudication that can shape outcomes. Conversely, where the DPA is housed or embedded within another entity such as inside Uganda's NITA-U, Ethiopia's ECA and Zimbabwe's POTRAZ, institutional conflicts of interest could weaken regulatory enforcement, especially where the parent entity is implementing or has key roles in DPI roll out.

²⁹⁰ Constitutional Court of Uganda. (2026, March 17). *Alternative Digitalk Limited and others v. Attorney General* (Consolidated Constitutional Petitions No. 34, 37 & 42 of 2022) [2026] UGCC 3. Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/judgement/ugcc/2026/3/eng@2026-03-17>; Uganda Communications Commission. (2026, January 14). Temporary suspension of public internet access and selected mobile services. <https://www.ucc.co.ug/wp-content/uploads/2026/01/Temporary-suspension-of-public-internet-access-and-mobile-services.pdf>

²⁹¹ World Bank. (2025, September 23). New World Bank program helps Zambia increase jobs through inclusive digital access. <https://www.worldbank.org/en/news/press-release/2025/09/23/new-world-bank-program-helps-zambia-increase-jobs-through-inclusive-digital-access>; Access Now / #KeepItOn. (2026). 2026 elections and internet shutdowns watch. <https://www.accessnow.org/campaign/2026-elections-and-internet-shutdowns-watch/>

²⁹² National Assembly of Zambia. (2025). Cyber Security Act, No. 3 of 2025. <https://www.parliament.gov.zm/node/12319>

²⁹³ World Bank. (2021). Digital economy for Zimbabwe: Country diagnostic report. <https://documents1.worldbank.org/curated/en/982981621880260112/pdf/Digital-Economy-for-Zimbabwe-Country-Diagnostic-Report.pdf>; United Nations in Zimbabwe. (2026, March 14). Zimbabwe unveils 2026–2030 AI strategy to advance inclusive digital transformation. <https://zimbabwe.un.org/en/311859-zimbabwe-unveils-2026%E2%80%932030-ai-strategy-advance-inclusive-digital-transformation>; Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. <https://zimtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE-2026-National-Budget-25-November-2025-final.pdf>

²⁹⁴ High Court of South Africa, Gauteng Division. (2024, January 16). *P.P.M. and others v. Minister of Home Affairs and others* (14238/21) [2024] ZAGPPHC 2. SAFLII. <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>

²⁹⁵ Kenyalaw. (2024, August 12). *Haki na Sheria Initiative v. Attorney General & 4 others* [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>

²⁹⁶ Supreme Court of Ghana. (2026, February 25). *Gorni v. Vodafone Ghana Ltd and others* (J4/40/2025) [2026] GHASC 19/20. Ghana Legal Information Institute. <https://ghalii.org/judgements/GHASC/2026/2/>

²⁹⁷ Community Court of Justice, ECOWAS. (2025, May 14). *L'Association des Utilisateurs des Technologies de l'Information et de la Communication & Ndiaga Gueye v. Republic of Senegal* (ECW/CCJ/APP/37/23; ECW/CCJ/JUD/29/25). <https://courtecawas.org/wp-content/uploads/2025/08/JUD-ECW-CCJ-JUD-29-25-ASSOCIATION-DES-UTILISATEURS-DES-TECHNOLOGIES-DE-L'INFORMATION-ET-DE-LA-COMMUNICATION-Other-vs-REPUBLIC-OF-SENEGAL-ENG.pdf>

²⁹⁸ Constitutional Court of Uganda. (2026, March 17). *Alternative Digitalk Limited and others v. Attorney General* (Consolidated Constitutional Petitions No. 34, 37 & 42 of 2022) [2026] UGCC 3. Uganda Legal Information Institute. <https://ulii.org/en/akn/ug/judgement/ugcc/2026/3/eng@2026-03-17>

The second category are legal conditions evident through existence and implementation of robust policy and legal frameworks for DPI, including data protection, cybersecurity and identity laws. They should have clear justiciable duties and obligations, incorporate international human rights standards, human rights due diligence and mandatory data protection impact assessments. Also, they should provide for non-discrimination, equal treatment, universal inclusion and analogue alternatives, accessibility and affirmative action standards, consumer protection, establish independent oversight bodies, require proactive disclosure of information regarding how data is used, promote open government, mandate meaningful multistakeholder participation, entrench rights to effective remedy and embed legal obligations and principles into the technical architecture such as inclusion-, privacy- and security-by-design.²⁹⁹

The technical conditions are important as the technical architecture directly shapes or determines the human rights outcomes. The adoption of open-source foundational software, such as the Modular Open Source Identity Platform (MOSIP) already deployed in Ethiopia and Uganda, could prevent proprietary vendor lock-in, ensure local code audibility, and support user-controlled credentials.³⁰⁰ Furthermore, deploying decentralized, federated data exchange architectures, such as X-Road / USP models in Tunisia could ensure source databases remain separated, preventing the creation of centralized, omni-surveillance state registers.³⁰¹ To be fully effective, these architectures must be complemented by open standards, transparent procurement, and baked-in data protection principles including granular consent, privacy-by-design and data minimisation.

Lastly, rights-respecting DPI will depend on robust civic and democratic conditions to ensure technology serves the public good rather than other purposes. A free and protected civic space is a mandatory prerequisite for DPI meaningful oversight and accountability. Independent investigative journalism, academic research, and active civil-society coalitions such as Katiba Institute and Nubian Rights Forum in Kenya, ISER and Unwanted Witness in Uganda, MISA Zimbabwe, Paradigm Initiative and SERAP in Nigeria, and AfricTivistes in Senegal provide the primary diagnostic, engagement, public awareness and litigation capacity to monitor implementation, audit systems, expose data breaches, challenge exclusion, and compel state compliance. State and bodies developing DPI should ensure meaningful participation of academia, civil society and the media in the DPI development lifecycle.

Kenya's example shows that participation should be assessed by timing and influence, not by the mere existence of consultation. On 14 September 2023, a coalition of 10 civil-society and community organisations urged the Government to halt the planned Maisha Namba rollout until there was a proper legal framework, meaningful nationwide public participation, accessible documentation, data protection and human rights impact assessment, and stronger inclusion safeguards.³⁰² Amnesty International Kenya's 16 September 2024 perception study subsequently found low public awareness, including limited information in Kiswahili, and called for stronger privacy, inclusion and digital-literacy measures.³⁰³ There are more recent signs of movement with the government's February 2026 National Data Governance Policy validation involving government, counties, private sector, academia, civil society and development partners, and the draft was later opened for public comment.³⁰⁴ Across Africa, election practice adds two additional enabling conditions: contestability and recoverability. Citizens, parties, observers and oversight bodies need enough information to test whether a system operated as claimed, while officials need a lawful way to continue participation when it did not.³⁰⁵ Hybrid paper-digital design can therefore be a mature resilience choice rather than a transitional stage.

299 Justice-Ready Digital Public Infrastructure: Building a Third Layer of Trust for Democratic Resilience <https://www.globalgovernance.eu/publications/justice-ready-digital-public-infrastructure-building-a-third-layer-of-trust-for-democratic-resilience>; Africa Nenda <https://africanenda.org/building-a-foundation-for-digital-public-infrastructure-in-financial-services>; Digital Public Infrastructure Through an Open Government Lens <https://africlaw.com/2026/02/11/digital-public-infrastructure-through-an-open-government-lens/>; Rights-Respecting Digital Public Infrastructure Principles <https://freedomonlinecoalition.com/rights-respecting-dpi-principles/>; Quad Principles for Development and Deployment of Digital Public Infrastructure <https://www.mea.gov.in/bilateral-documents?dtl/38329/Quad+Principles+for+Development+and+Deployment+of+Digital+Public+Infrastructure>

300 Building Digital Infrastructure Through Open Source and Its Possibilities <https://unu.edu/article/building-digital-infrastructure-through-open-source-and-its-possibilities>

301 Digital Public Infrastructure And Development: A World Bank Group Approach <https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf>

302 Kenya Human Rights Commission et al. (2023, September 14). Human rights organizations urge government to expand consultations and safeguards before Unique Personal Identifier/Maisha Namba rollout. <https://khrc.or.ke/press-release/human-rights-organizations-urge-government-to-expand-consultations-and-safeguards-before-unique-personal-identifier-maisha-namba-rollout/>

303 Amnesty International Kenya. (2024, September 16). Ready or not? Citizens' perspectives on Maisha Namba. <https://www.amnestykenya.org/aik-perception-study-report-ready-or-not-citizens-perspectives-on-maisha-namba/>

304 Ministry of Information, Communications and the Digital Economy, Kenya. (2026, February 6). Government moves to strengthen Kenya's data governance framework. <https://ict.go.ke/government-moves-strengthen-kenyas-data-governance-framework>; Ministry of Information, Communications and the Digital Economy, Kenya. (n.d.). Public participation: Draft final National Data Governance Policy, May 2026. Retrieved September 11, 2026, from <https://ict.go.ke/call-public-participation>

305 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>; International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; African Commission on Human and Peoples' Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achprres655lxxvi-2026>

4.5.3 Roles of Stakeholders in Improving DPI Governance

Governments, regulators, private actors, development partners and civil society play a major role in undertaking and facilitating efforts to improve DPI governance. Rights-respecting DPI governance requires distributing specific, non-substitutable responsibilities across all actors in the ecosystem, ensuring that state duties are not diluted when functions are outsourced to private intermediaries.

Governments and public institutions are the primary duty bearers under international law. Of the stakeholder groups, their roles are clearest in law but less coordinated in practice. Ideally, governments should establish the legal statutory foundations and purposes for every DPI pillar; guarantee offline or non-digital alternative channels for digital-only essential services; invest in and fund last-mile digital infrastructure and protect civic space required for public scrutiny. Regulators and data protection authorities should transition from reactive complaint handling to proactive technical auditing of public and private databases. They also need to enforce breach reporting and publish binding enforcement decisions, audit reports, and complaint statistics in accessible language to build transparent jurisprudence. Also, courts should remain able to independently review both the design and implementation of DPI.

Private technology providers, telecom operators, and payment firms should ensure their practices align with the UN Guiding Principles on Business and Human Rights (UNGPs), including conducting and publishing project-specific Human Rights Due Diligence (HRDD) reports prior to contract execution, incorporating privacy principles such as privacy- and security-by-design, disclosing government data requests, and establishing operational grievance mechanisms for technical and service failures.

Development partners and international financiers such as the World Bank, Gates Foundation, UNDP, and Co-Develop, should condition loan disbursements and project milestones on verified inclusion, published HRIAs/DPIAs, and effective remedy mechanisms, rather than relying exclusively on aggregate enrolment totals or transaction volumes. DIAL's 2025 research found that civil society's awareness and role have grown in significance around DPI in Africa but remain underdeveloped, as they are often excluded from its design, governance, oversight and critical stages of the DPI lifecycle.³⁰⁶ The progressive direction for civil society, media, and academia should be to move scrutiny upstream by participating in the DPI development life cycle from policy and architecture design to procurement and monitoring and evaluating implementation. They should also maintain and build capacity in strategic litigation, investigative reporting and research to document the lived experiences of communities, audit DPI and monitor DPI procurement.

Across Africa, the emerging division of responsibility should also preserve electoral independence. Identity agencies should provide limited, lawful verification services. EMBs should retain custody and decision-making authority over electoral registers, and data-protection authorities should supervise processing. Vendors should meet contractual and UNGP duties, and telecoms should protect availability and lawful access.

4.5.4 Roles of International and Regional Bodies in Establishing Minimum Standards for Rights-Respecting DPI

African regional and continental bodies play a vital role in establishing minimum human-rights baselines, harmonizing data protection standards, and providing external judicial recourse. The African Union and Regional Economic Communities (RECs) have over the years established a robust normative base. The continental normative frameworks are becoming more detailed, but binding coverage and implementation at the domestic level remain uneven. As of 2 February 2026, 20 states had ratified/deposited the Malabo Convention, including Ghana, Senegal and Zambia as parties, while Nigeria, South Africa and Tunisia had signed but not ratified.³⁰⁷ The AfCFTA Digital Trade Protocol, African Digital Compact, Continental AI Strategy and 2025 data-provision guidelines broaden the policy environment for interoperability, inclusion and trusted data use.³⁰⁸ Regional bodies must incentivize states to pursue full ratification and translate continental principles into binding model procurement clauses, DPIA templates, and vendor transparency standards.

³⁰⁶ Digital Impact Alliance. (2025, October 9). The people's network: Civil society organizations in DPI development in Africa. https://dial.global/wp-content/uploads/2025/10/CSOs_DPI_Engagement_Final.pdf

³⁰⁷ African Union. (2026, February 2). Status list: African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf

³⁰⁸ African Union. (2024, August 9). Continental Artificial Intelligence Strategy. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>; African Union. (2024, August 9). African Digital Compact. <https://au.int/en/node/44005>; African Union. (2024, February 18). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. https://opendata.pap.au.int/akn/aa-au/act/protocol/2024/free_trade_area_on_digital_trade/eng@2024-02-18/source.pdf; African Union. (2025, May 22). Guidelines for integrating data provisions in protocols on digital trade. <https://au.int/en/documents/20250522/guidelines-integrating-data-provisions-protocols-digital-trade>

Across Africa, the AU Digital ID Interoperability Framework and ACHPR Resolution 655 provide complementary directions. The promotion of technical interoperability should be paired with minimisation, trust and accountability, while electoral processes require independent EMBs, open communications and effective redress.³⁰⁹ The remaining gap is ‘governance interoperability’, compatible rules on audit, correction, access and remedy wherever foundational systems cross institutional or national boundaries.

Regional judicial recourse and enforcement can provide essential external remedy especially when domestic judicial or regulatory channels are captured or unresponsive. South Africa and Kenya show the value of independent courts and regulators to pause, review or correct state action. However, South Africa still faces frontline and inequality problems and Kenya’s litigation is often corrective rather than preventive, Ghana provides a recent example of judicial enforcement of the constitutional right to privacy, including an award of damages, although remedy has been individual rather than system-wide. Senegal shows that a regional court - ECOWAS - can supply a remedy when domestic routes are inadequate. The East African Court of Justice (EACJ), and the African Court on Human and Peoples’ Rights (ActHPR) also provide secondary judicial recourse opportunities.

Continental frameworks will remain significant as many future DPI functions will cross borders through trade, payments, identity verification and data flows. The Malabo Convention, African Digital Compact, AfCFTA Digital Trade Protocol, AU Data Policy Framework and Universal DPI Safeguards Framework can help establish a common baseline and standards.³¹⁰ However, the comparison across the 11 countries shows that principles need robust institutions behind them to ensure public reporting, independent review, compatible correction rules, and regional remedies that can actually be used.

The strongest enabling conditions appear where safeguards are plural and contestable: courts, independent regulators, civil society, transparent design, and practical alternatives. South Africa and Kenya currently show strong independent institutional checks. Ghana and Nigeria have important regulatory capacity but need stronger DPI-specific implementation. Senegal offers a significant regional-remedy precedent that West African nations can draw on. Earlier-stage or more weakly supervised systems still have an opportunity to build these conditions before interoperability becomes deeply entrenched

309 African Commission on Human and Peoples’ Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achpres655lxxxvi-2026>; African Union Commission. (2023, December 11). AU interoperability framework for digital ID. https://www.au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf

310 12. UNDP. (2026). How the DPG Standard and Universal DPI Safeguards Framework are charting a safe and inclusive digital future. <https://www.undp.org/digital/blog/how-dpg-standard-and-universal-dpi-safeguards-framework-are-charting-safe-and-inclusive-digital-future>; UNDP. (2024). Universal DPI Safeguards Framework: A guide to building safe and inclusive DPI for societies (updated 2025). <https://www.undp.org/publications/universal-safeguards-digital-public-infrastructure>

5.0 Discussion:

Impact of DPI on Digital Rights, Civic Participation, and Democratic Governance

This section discusses the impact that DPI has on digital rights, civic participation and democratic governance in Africa. As seen across the countries, DPI is not a set of neutral technical tools. Instead, it functions as a rights and power multiplier. On one hand, it increases the operational capacity of the state to identify, authenticate, transact with, and deliver services to citizens, and on the other hand, it expands the state's legibility, surveillance surface area, and coercive control over the population. When foundational identity, retail payment switches, and inter-agency data exchange platforms are integrated without matching, independent safeguards, the resulting ecosystem alters the constitutional balance of power between states, commercial technology intermediaries, and individual rights-holders.

As shown in the preceding sections, DPI is expanding the state's capacity faster than it is producing uniform rights or democratic outcomes. DPI is developing in an environment where regulatory and data-protection institutions, civic space, election rules, and judicial oversight are also evolving. The outcomes and impact of DPI are also mixed. A country with weak safeguards can improve. A country with good law can regress. Also, a system that carries limited risk while optional may become far more consequential once it is made mandatory or linked to additional services. The human rights and democratic quality of DPI will be shaped by the decisions made by the responsible actors, as well as by how quickly systems are built. Ultimately, the quality of the outcomes depends on the design choices, political context, institutional independence, civic space, and whether a remedy is available when systems fail or are misused.

5.1 Equality and Inclusion

Across the countries, state authorities justify DPI expansion through narratives of administrative modernisation, financial inclusion, anti-fraud efficiency, and social grant targeting. However, empirical findings reveal that making digital identity credentials compulsory for essential services converts administrative infrastructure into a rights chokepoint. When foundational digital ID, SIM card ownership, and bank account access are legally or operationally linked, an initial enrolment failure, biometric read error, or administrative restriction can trigger exclusion cascading across multiple systems, such as in healthcare, telecommunications, social safety, banking and civic participation across an individual's entire life.

Inclusion gains are evident where people already have reliable identity records, devices, connectivity and service channels. Inequality is pronounced where those conditions become mandatory but remain unequally distributed. Cascading exclusion is most visible in countries where mandatory policies have generated large-scale rights disruptions. The study found substantial convenience and financial-access gains in Ghana, South Africa, Kenya and Nigeria, while Uganda and Ethiopia show how documentation or authentication barriers can affect several services once identity becomes the primary access gateway. In Ethiopia, with the mandatory requirement for Fayda ID for opening bank accounts, subsequent reporting has shown that women and refugee community enrolments remained low. In Uganda, studies have shown that one-third of the adult population lacked a national ID due to NIRA enrollment bottlenecks, and consequently, 50,000 elderly persons were excluded from state pensions. Further, SIM deactivation processes in Ghana and Nigeria have resulted in multiple connected financial services being affected. Also, as government systems such as in Tunisia and Egypt require digital IDs linked to registered SIM cards, then those without ID or SIM cards cannot essentially access financial or essential government services.

The study found no distinction between countries with only benefits and other countries with harms, as both often occur in the same system. Moreover, once authorities require digital identity as mandatory to access to certain services, then technical glitches, logistical card backlogs, and geographic digital divides can also become structural engines of socio-economic and political disenfranchisement. Key populations facing such exclusion include manual agricultural labourers with worn fingerprints such as cocoa farmers in Ghana, rural agricultural workers in Ethiopia, elder manual labourers in Nigeria, who face permanent authentication barriers due to biometric failures. Women and refugees in Ethiopia, marginalised Nubian and Somali border communities in Kenya, also face discriminatory enrolment and vetting processes.

Across Africa, deeper DPI–election convergence could make political equality more dependent on the quality of civil and identity administration. The progressive pathway is ensuring continuous, inclusive updating with easy correction and alternatives. The adverse pathway is automatic disenfranchisement when an upstream record is wrong or inaccessible. Ghana’s 2024 decision to retain guarantor registration and Ethiopia’s hybrid 2026 registration illustrate how policy can preserve an exception as digital systems expand.³¹¹

The democratic significance is that equal citizenship is partly experienced through administration. Administrative inequality can become political inequality, especially where some people can authenticate once and move easily through public systems and services while others have to repeatedly prove identity, travel further, pay more, or wait longer for correction. Progressive systems therefore need to measure not only enrolment totals but successful use, correction time, fallback access, and exclusion by gender, disability, age, income, and geography.

If the current pattern continues, the inclusion question will move from initial enrolment to cumulative dependence. More services will become easily accessible for people whose identity records are accurate and whose devices and connectivity work, while people who struggle to register or authenticate may lose access to a growing number of services at once. The risk is a two-tier form of digital citizenship where there is administrative convenience for the well-connected and exclusion for those already at the margins who have to endure repeated proof, travel, high cost, and delay. A more inclusive direction is visible where governments retain assisted or non-digital channels and measure failed authentication, correction time, and exclusion rather than enrolment alone.

5.2 Privacy, Interoperability and State Su

The primary technical dividend of DPI is touted as the seamless interoperability of standardised data-exchange layers such as Kenya’s *GavaConnect*, Senegal’s *Jokkoo/PINS*, Tunisia’s *TunXRoad*, Egypt’s Government Service Bus, South Africa’s *MzansiXchange*, Uganda’s *UGHub*, and Zambia’s *ZamConnect*. On one hand, they offer visibility that can deliver undeniable administrative benefits by breaking down agency silos, enabling automated information sharing between government ministries, businesses and law enforcement, supporting fraud control and improving service coordination. On the other hand, evidence demonstrates that without strict purpose limitation, role-based access controls, and immutable, independently audited access logs, interoperability can act as a state surveillance and legibility amplifier that expands the potential for profiling, surveillance and function creep or secondary use.

Digital transformation efforts are now connecting previously separate administrative and transactional databases such as foundational civil registers, biometric identity vaults, subscriber mobile location records, tax files, and mobile money switches, and interoperability can convert these isolated datasets into an integrated, searchable national surveillance database. This can reconfigure state power, expanding state visibility into people’s private lives, while creating a high risk of function creep.

For example, in Uganda, the national identity project was originally conceived as a security project and now the *Ndaga Muntu* identity, telecom, and government-data systems are increasingly interconnected.³¹² In Egypt and Tunisia, government services and financial identity are expanding within a restrictive civic environment;³¹³ and in Zimbabwe, future plans for Project Pangolin would add a new national data layer to an already centralised telecommunications and data-protection oversight structure.³¹⁴ In Ghana, a dispute in April 2025 resulted in NIA disconnecting the Ghana Revenue Authority from its identity verification service over an unpaid debt.

In Nigeria, an investigative breach exposed that up to 43 million NIN records were being illegally offered for commercial sale on unverified data-broker websites for as little as ₦100 (USD 0.075) per query, even as the NIMC database is interlinked with Bank Verification Numbers (BVN), tax registries, and telecom subscriber data via the *NINAuth* verification rail and the Nigerian Data Exchange (NGDX). In addition, the convergence of foundational identity databases with physical smart-city surveillance networks and data exchange hubs represents the most direct integration of DPI into state policing apparatuses. So far, at least 21 African

311 Intergovernmental Authority on Development. (2026, June 3). IGAD Election Observation Mission to Ethiopia’s 7th General Election: Preliminary report. <https://igad.int/igad-election-observation-mission-to-the-7th-general-election-of-the-federal-democratic-republic-of-ethiopia-held-on-monday-june-1-2026-preliminary-report/>; Ghana News Agency. (2024, March 7). Election 2024: EC shelves use of Ghana Card as sole identity document. <https://gna.org.gh/2024/03/election-2024-ec-shelves-use-of-ghana-card-as-sole-identity-document/>

312 National Information Technology Authority–Uganda (NITA-U) on X, <https://x.com/NITAUGanda1/status/2092477136774807888>

313 State Information Service, Egypt. (2026, July 21). Communications Minister: Egypt to offer more than 270 digital government services by end-2026. <https://sis.gov.eg/en/media-center/news/communications-minister-egypt-to-offer-more-than-270-digital-government-services-by-end-2026/>; Central Bank of Egypt. (2025, November 16). PAFIX 2025: Digital Financial Identity platform (Haweya). <https://www.cbe.org.eg/en/news-publications/news/2025/11/16/18/47/pafix-2025>

314 Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. https://zimtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE_2026-National-Budget_25_November_2025-final.pdf

countries currently host or are planning smart city and intelligent urban projects. These examples do not establish that DPI itself is being used for political surveillance in every case. They highlight the potential consequences of weak access controls as more data can be linked.

Gaps in independent oversight can also arise where data protection authorities are hosted or mandates are assigned to sector regulators as in Uganda, Ethiopia and Zimbabwe, which can create structural conflict of interest. Also, several countries have lawful interception laws such as in Zambia, some of which compel installation of real-time interception capabilities, with limited oversight, could undermine data protection.

Importantly, the next privacy frontier will be inference rather than collection alone. Reusable identity, transaction histories, location, communication metadata and electoral or civic information can be combined and when coupled with AI systems, can rapidly infer behaviour even where each dataset was lawfully collected for a separate purpose.³¹⁵ The increased development and use of AI tools increase the importance of purpose limitation, model and data provenance, bias testing, explainability, human review and auditable access.³¹⁶

Therefore, the evidence supports a cautious conclusion that capability is not the same as abuse. The governance question is whether each query or linkage has a lawful purpose, limited access, auditable logs, retention controls, independent authorisation where required, and a route for the person affected to challenge misuse. This distinction helps avoid attributing every civic-space problem to DPI while still recognising that integrated infrastructure can increase the consequences of abuse.

Looking ahead, the main privacy issue is likely to shift from whether information is stored in one central database to who can query, link, and infer from distributed databases. Federated exchange can reduce wholesale copying of data, but it does not by itself prevent pervasive visibility if many agencies can make queries without narrow purposes, logging, or independent review. As exchange layers mature in Ghana,³¹⁷ Senegal,³¹⁸ South Africa,³¹⁹ and Uganda,³²⁰ and as Zimbabwe develops Project Pangolin,³²¹ auditability and purpose limitation will become as important as database location. Tunisia's IUC law offers a useful design marker by giving citizens a right to see which actions have been performed on their unique identifier, the organisations that have performed them, or used it.³²² In more restrictive civic environments, the same technical capacity can lower the cost of profiling political or social groups even where no abuse has yet been documented.

Taken together, the comparative evidence across all eleven study countries reveals that state visibility in the DPI era is no longer defined merely by whether personal information is stored in a single central vault. Instead, mass visibility is produced at the connections between systems, which include the application programming interfaces (APIs), federated data exchange hubs, eKYC verification queries, and payment switches that link identity to daily economic and civic life. When states expand these digital connections faster than they establish independent data protection authorities, mandatory access logging, strict purpose limitation, and warrant-based judicial oversight, DPI ceases to function as a neutral engine of administrative efficiency. Instead, it becomes an infrastructure of pervasive state legibility, where a citizen's every transaction, movement, and communication leaves a permanent, traceable, and potentially punitive record before the state.

³¹⁵ International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>

³¹⁶ African Union. (2024, August 9). Continental Artificial Intelligence Strategy. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>

³¹⁷ National Information Technology Agency, Ghana. (2025). Data Harmonisation Bill: Proposed National Data Exchange Platform and interoperability framework. <https://nita.gov.gh/wp-content/uploads/2025/NITA-Data-Harmonisation-Bill.pdf>

³¹⁸ Ministry of Communication, Telecommunications and the Digital Economy, Senegal / Jokkoo. (2026). National interoperability platform (PINS/Jokkoo). <https://www.pins.sn/>; Ministry of Communication, Telecommunications and the Digital Economy, Senegal / Jokkoo. (2026, January 16). Inter-ministerial and interoperable data-exchange platform of Senegal. <https://pins.sn/actualites/2026-01/plateforme-interministerielle-et-interoperable-dechange-de-donnees-du-senegal>

³¹⁹ National Treasury, South Africa. (2025, October 9). MzansiXchange pilot launch. <https://mzansixchange.treasury.gov.za/pilot/>

³²⁰ National Information Technology Authority–Uganda (NITA-U) on X, <https://x.com/NITAUGanda1/status/2092477136774807888>

³²¹ United Nations in Zimbabwe. (2026, March 14). Zimbabwe unveils 2026–2030 AI strategy to advance inclusive digital transformation. <https://zimbabwe.un.org/en/311859-zimbabwe-unveils-2026%E2%80%932030-ai-strategy-advance-inclusive-digital-transformation>; Government of Zimbabwe, Ministry of Finance, Economic Development and Investment Promotion. (2025, November 25). 2026 national budget. https://zimtreasury.co.zw/wp-content/uploads/2025/11/NEW-THE_2026-National-Budget_25_November_2025-final.pdf

³²² Tunisia Legal Database / DCAF. (2020, May 12). Decree-Law No. 2020-17 on the Unique Citizen Identifier. <https://legislation-securite.tn/latest-laws/decret-loi-du-chef-du-gouvernement-n-2020-17-du-12-mai-2020-relatif-a-lidentifiant-unique-du-citoyen/>

5.3 DPI and Election Integrity

As DPI is increasingly being connected to essential public services, they are also being connected through the same telecommunications networks to electoral technology systems. Foundational ID databases serve as the primary verification registers for generating voter registers and authenticating voters at polling stations. Egypt derives the voter database from national-ID data.³²³ Ethiopia used *Fayda*-enabled *Mirchaye* registration in 2026 while retaining manual registration.³²⁴ Ghana preserved non-Ghana-Card registration routes for the 2024 cycle.³²⁵ Kenya is pursuing Integrated Population Registration System (IPRS) verification while keeping the voter register under IEBC control.³²⁶ Nigeria is deepening INEC–NIMC cooperation while the 2026 Electoral Act retains a signed paper result as fallback.³²⁷ Senegal’s biometric credential is closely tied to voting.³²⁸ South Africa combines population-register validation, voter management devices (VMDs), and paper fallback while considering future digital-ID interoperability.³²⁹ Tunisia uses automatic registration.³³⁰ Uganda draws voter-register data from the national database.³³¹ Zambia and Zimbabwe retain more functionally distinct biometric voter registers.³³² While these are different architectures in operation, their use makes identity governance more relevant to democratic participation.

Across Africa, the information environment is now part of electoral infrastructure. Voters need connectivity not only for registration or results, but also for journalism, election observation, political organising, and access to information. EMBs need connectivity for coordination and election results transmission. ACHPR Resolution 655 of 13 March 2026 calls for uninterrupted telecommunications and stronger responses to disinformation, urging states to protect election integrity without turning network control or vague speech rules into tools of political restriction.³³³ The convergence is further complicated by state-imposed internet disruptions during elections to control information flows. This creates a self-defeating operational paradox as disabling connectivity to suppress political speech also paralyses the dependent infrastructure needed for eKYC, mobile money and essential online services. The most direct example is Uganda, where the UCC issued its suspension directive on 13 January 2026, two days before polling, after a recommendation from the Inter-Agency Security Committee, and restored public internet on 18

- 323 National Election Authority, Egypt. (2014). Law No. 45 of 2014 on the Exercise of Political Rights (Arts. 13–14). <https://parliament2015.elections.eg/imag->
- 324 National Election Board of Ethiopia. (2026, January 6). NEBE inaugurates first-of-its-kind voter and candidate registration system. <https://nebe.org.et/am/node/1222>; Intergovernmental Authority on Development. (2026, June 3). IGAD Election Observation Mission to Ethiopia’s 7th General Election: Preliminary report. <https://igad.int/igad-election-observation-mission-to-the-7th-general-election-of-the-federal-democratic-republic-of-ethiopia-held-on-monday-june-1-2026-preliminary-report/>
- 325 Electoral Commission of Ghana. (n.d.). Voter registration. Retrieved September 13, 2026, from <https://ec.gov.gh/registration/>; Ghana News Agency. (2024, March 7). Election 2024: EC shelves use of Ghana Card as sole identity document. <https://gna.org.gh/2024/03/election-2024-ec-shelves-use-of-ghana-card-as-sole-identity-document/>
- 326 Independent Electoral and Boundaries Commission, Kenya. (2022). Post-election evaluation / register of voters report. <https://www.iebc.or.ke/uploads/resources/pabjKTV6Xa.pdf>; Independent Electoral and Boundaries Commission, Kenya. (2026, February 16). Statement on voter-register integrity and proposed secure
- 327 National Assembly of Nigeria. (2026, February 18). Electoral Act, 2026 (Act No. 1). ss 60 <https://nass.gov.ng/documents/download/11248>; Independent National Electoral Commission, Nigeria. (2025, September 3). Remarks on INEC–NIMC collaboration, continuous voter registration and the long-term relationship between the citizenship and voter registers. <https://www.inecnigeria.org/remarks-by-the-chairman-independent-national-electoral-commission-inec-prof-mahmood->
- 328 African Union Election Observation Mission. (2024, April 10). Final report on the presidential election of 24 March 2024 in Senegal. <https://au.int/en/node/44059>
- 329 Electoral Commission of South Africa. (2024). 2024 national and provincial elections report. <https://www.elections.org.za/content/Documents/Election-reports/National-and-Provincial-Elections/2024-National-and-Provincial-Elections-Report/>; Schreiber, L. (2025, March 10). Address by Home Affairs Minister at the IEC Conference and Exhibition on Electronic Voting Technologies [Speech transcript]. Polity. <https://www.polity.org.za/article/sa-leon-schreiber-address-by-home-affairs-minister-iec-conference-and-exhibition-on-electronic-voting-technologies-10032025-2025-03-11>
- 330 International Foundation for Electoral Systems. (2024). Elections in Tunisia: 2024 presidential elections. <https://www.ifes.org/tools-resources/elec->
- 331 Electoral Commission of Uganda. (2025, December 24). The Electoral Commission (Adoption and Manner of Use of Biometric Voter Verification System) Regulations, 2025 (S.I. No. 98 of 2025). https://www.ec.or.ug/sites/default/files/docs/The%20Electoral%20Commission%20%28Adoption%20and%20Manner%20of%20Use%20of%20Biometric%20Voter%20Verification%20System%29%20Regulations%2C%202025_Edited.pdf; Electoral Commission of Uganda. (2026, January 15). Guidance on verification of voters at polling stations. <https://www.ec.or.ug/election/20252026-general-elections?page=8>
- 332 African Union Election Observation Mission. (2021, August 14). Preliminary findings on Zambia’s 12 August 2021 general elections. <https://au.int/en/press-releases/20210814/aeom-statement-preliminary-findings-zambias-2021-general-elections>; Zimbabwe Election Support Network. (2023). 2023 harmonised elections report. <https://www.zesn.org.zw/wp-content/uploads/2015/10/ZESN-2023-Harmonised-Election-Report.pdf>
- 333 African Commission on Human and Peoples’ Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://>

January 2026.³³⁴ Also, in Kenya, the internet shutdown imposed during the #RejectFinanceBill protests on 25 June 2024 affected access to essential and financial services in Uganda, Rwanda, and Burundi.³³⁵

In particular, the comparison across the countries shows both progress and continuing risk. Ghana's 7 December 2024 election and South Africa's 29 May 2024 election used digital technologies without an election-period internet shutdown. Access Now detected no election-period shutdown in Ethiopia on 1 June or in Zambia on 13 August 2026.³³⁶ Nonetheless, the absence of a shutdown, while a meaningful but narrow indicator, should not be treated as proof of overall electoral quality.

Ghana, Nigeria, and Kenya's previous experiences have shown that technology can improve verification and transparency yet remain vulnerable to connectivity, implementation, and trust problems. Nigeria's Electoral Act 2026, like Kenya's Elections Act, requires presiding officers under section 60(3) to transmit polling-unit results electronically to the IReV portal after Form EC8A is signed and stamped, while retaining the signed paper form as the primary collation source if communication failure makes transmission impossible.³³⁷ INEC's current election calendar lists 16 January and 6 February 2027 for the principal 2027 general-election polls,³³⁸ while Kenya is expected to go to the polls on 10 August 2027.³³⁹ If these models work as intended, they could strengthen transparency and auditability. If connectivity, device performance, institutional communication or public access fails, a technical problem can rapidly become a legitimacy problem, as witnessed in Kenya's nullified 2017 presidential election.³⁴⁰ The democratic safeguard is therefore not "more election technology" alone, but transparent fallback rules, independent observation, open connectivity and timely publication of discrepancies.

5.4 Accountability Deficit and Remedy

Assessing the developments in the countries on the basis of the UNGPs shows that formal legislative enactment has drastically outpaced operational enforcement and remedy. Under Pillar 1 (State Duty to Protect), whereas countries have developed identity, data protection, cybersecurity and e-government laws, regulatory enforcement is compromised by structural conflicts of interest, facing data protection bodies in Ethiopia, Uganda and Zimbabwe.

Under Pillar 2 (Corporate Responsibility to Respect), publicly documented UNGP-aligned Human Rights Due Diligence (HRDD) reports by private technology vendors engaged in DPI development are either non-existent or limited. French vendor IDEMIA adopted an amended Corporate Vigilance Plan following litigation by civil society.³⁴¹ Under Pillar 3 (Access to Remedy), there is improvement in some jurisdictions but it remains weak. Ordinary citizens facing individual DPI service failures or privacy violations almost never receive administrative remedy or financial compensation. Instead, strategic litigation brought by well-resourced civil society organisations before independent courts has served as the primary de facto safeguard.

For example, South Africa's Gauteng High Court decision of 16 January 2024 constrained unfair ID blocking for 300,000 affected persons. The ECOWAS Court ruled against Senegal's 2023 shutdowns on 14 May 2025. Ghana's Supreme Court awarded a privacy remedy on 25 February 2026 for unauthorised Ghana Card-linked telecom/mobile-money use. Kenya's High Court halted the rollout of Huduma Namba for failure to conduct a DPIA. Uganda's Constitutional Court struck down the Computer Misuse (Amendment) Act and criminal-libel provisions on 17 March 2026.

Across Africa, the weakness of remedy is evident where time-sensitive rights are involved. Election administration requires correction before registration closes, fallback on polling day, and preservation of evidence for challenge after results are declared.³⁴²

334 Uganda Communications Commission. (2026, January 14). Temporary suspension of public internet access and selected mobile services. <https://www.ucc.co.ug/wp-content/uploads/2026/01/Temporary-suspension-of-public-internet-access-and-mobile-services.pdf>; Uganda Communications Commission. (2026, January 18). Public update: Restoration of public internet access. <https://www.ucc.co.ug/public-update-18th-january-2026-press-briefing-to-update-the-country/>

335 CIPESA. (2024, September 27). 2024 State of Internet Freedom in Africa report unveils the promises and challenges of technology in African elections. https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf

336 Access Now / #KeepItOn. (2026). 2026 elections and internet shutdowns watch. <https://www.accessnow.org/campaign/2026-elections-and-internet-shutdowns-watch/>

337 National Assembly of Nigeria. (2026, February 18). Electoral Act, 2026 (Act No. 1). ss 60 <https://nass.gov.ng/documents/download/11248>

338 Independent National Electoral Commission, Nigeria. (n.d.). Upcoming elections. Retrieved September 13, 2026, from <https://www.inecnigeria.org/upcoming-elections/>

339 IEBC (2026, September 14), Publication of Notice of General Election, https://www.iebc.or.ke/news/?PUBLICATION_OF_NOTICE_OF_GENERAL_ELECTION

340 BBC. (2017, September 1). Kenya presidential election cancelled by Supreme Court <https://www.bbc.com/news/world-africa-41123329>

341 NGOs and IDEMIA agree to Vigilance Plan Improvements in Settlement over Kenyan Digital ID Human Rights Challenge <https://khrc.or.ke/press-release/ngos-and-idemia-agree-to-vigilance-plan-improvements-in-settlement-over-kenyan-digital-id-human-rights-challenge/>

342 International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>; International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

DPI systems for health, social benefits, identity or finance can adopt the same principle that remedies should be designed to prevent foreseeable interruption, not only compensate after harm.

While these cases are progressive, they also show the limits of legal victories. South Africa required follow-up litigation over implementation; Uganda's March 2026 expression judgement did not resolve the separate June 2025 national-ID exclusion dispute; and Ghana's individual privacy remedy did not by itself resolve broader questions about verification, access, and system governance. Effective remedy therefore requires not only a judgement or complaint channel but timely implementation, affordable access, and correction that reaches every connected service and affected individual.

The future risk is a widening mismatch in speed. A state or private intermediary may be able to verify or deny access in seconds while a citizen takes days, months or years of litigation to correct the underlying record. Nigeria's recent regulatory experience illustrates a related institutional risk. The Nigeria Data Protection Commission's 18 February 2025 Final Order against Meta imposed a USD 32.8 million remedial fee and corrective directions, but a settlement dated 30 October and adopted by the Federal High Court on 3 November 2025 removed the fee while retaining compliance commitments, and the terms became publicly clearer only through reporting in April 2026.³⁴³ While the example is not DPI-specific, it shows why future accountability should be measured by final outcomes, implementation and transparency rather than enforcement announcements alone.

5.5 Participation and Contestability by Citizens

Citizen agency is stronger where people and civil society can influence rules before deployment and challenge them after deployment and during implementation. Kenya's identity litigation, Senegal's regional case, South African civil-society litigation, and Ghana's 2026 privacy judgement show that contestability can change outcomes. Yet DIAL's 2025 research indicates that African civil society is still commonly brought into DPI debates after core design choices have been made.³⁴⁴

Across Africa, public verifiability is a distinct form of participation. Election systems demonstrate that consultation is insufficient if parties, observers, journalists, or civil society cannot see the rules, test relevant components, reconcile digital outputs to human-readable records, or obtain timely incident and election information. DPI governance can borrow this emphasis on observable evidence without exposing sensitive security details or personal data.

If participation remains mainly reactive, the gap between system design and citizen agency will widen as DPI becomes harder to change after integration. Consultation after procurement or after a mandatory-use decision is less capable of correcting architecture than participation before purpose, data fields, authentication rules, and vendor terms are fixed. The more promising future direction is visible in systems that institutionalise civil-society and multistakeholder participation throughout design, pilot, expansion, and evaluation, with particular representation from traditionally marginalised or excluded groups who are often most likely to face documentation, disability, gender, language, or geographic barriers.

5.6 Interoperability Multiplies both Public Value and Systemic Risk

Interoperability multiplies the quality of the underlying rules. Where records are accurate, access is lawful, and alternatives exist, data exchange can reduce duplication and improve service delivery. Where records are wrong, mandatory or poorly supervised, the same integration can spread exclusion or misuse across institutions. Ethiopia, Uganda, Ghana, Nigeria and Kenya show how deeper linkage of databases and records can increase both potential value and systemic consequences.

Across Africa, the election cases show that interoperability can become constitutional. Once an identity API or population register materially determines access to the election, choices about source data, matching thresholds, query design, logging, and correction affect political equality. Selective disclosure and minimum-attribute verification are therefore preferable to broad copying or open-ended linking of foundational and electoral databases.

Recent developments in Kenya could elevate these risks as government services move from separate portals toward APIs and sectoral exchange systems. Consequently, the relevant privacy question is not 'where is the central database?' but 'which institution or application can query which record, for what purpose, under whose authority, and how can a person see and correct the resulting data flow?' *GavaConnect* and the health-data exchange regime point toward a future in which consequential DPI

³⁴³ Premium Times. (2026, April 26). Inside Nigeria's settlement of the NDPC's US\$32.8 million Meta remedial fee. <https://www.premiumtimesng.com/news/headlines/873350-exclusive-inside-nigerias-deal-to-write-off-32-8-million-fine-against-meta.html>

³⁴⁴ Digital Impact Alliance. (2025, October 9). The people's network: Civil society organizations in DPI development in Africa. https://dial.global/wp-content/uploads/2025/10/CSOs_DPI_Engagement_Final.pdf

decisions may occur in machine-to-machine transactions that citizens never see. If audit logs, purpose limitation, identity correction, and independent oversight mature alongside the APIs, this can reduce duplication and improve service continuity. If they lag, exclusion or unlawful access can be entrenched more quickly across institutions.

Overall, the key governance question is whether safeguards interoperate as well as databases do. A correction accepted by the identity authority should propagate to the connected services. High-risk access should leave an auditable trail; and users should not have to navigate several agencies to discover which system caused an adverse decision. This is one area where technical progress is ahead of governance across the study countries.

Systemic risk can also extend beyond data interoperability. Public systems share mobile operators, cloud control planes, authentication services, cable routes, data centres, or power. A failure or order directed at one common dependency can interrupt several connected or dependent services. Hence, resilience assessments should map these dependencies and test whether backups are physically, operationally and contractually independent. Moreover, successful enrolment will not automatically establish access to services if repeat authentication is unaffordable, the device or interface is unsuitable, or an outage prevents completion. The relevant desirable outcome will be improved affordable service completion rates across users and locations, including where they are assisted or through low-bandwidth and offline channels.

Several developments in the past year show that cumulative risk is also moving from theory into system design. Tunisia made Mobile ID mandatory from 1 July 2026 for investors declaring projects through approved digital platforms, demonstrating how an optional credential can rapidly become a sectoral gateway. Zimbabwe's National AI Strategy 2026–2030, formally launched in March 2026, identifies Project Pangolin as a national AI and data platform, whose implementation shall be phased from foundation-building in 2026, through scaling in 2027–2028, to ecosystem maturation in 2029–2030. South Africa's MzansiXchange and functional Digital ID are likewise intended to move from pilot and phased rollout toward wider use. If these trajectories continue, the central governance question will be whether correction, audit, lawful-access rules, and non-digital alternatives are built before interdependence becomes difficult to undo.

5.7 Digital Sovereignty and Dependence on Vendors and Financiers

Governments are giving greater policy weight to digital sovereignty, aiming to build local DPI rails, secure data location, build domestic cloud data centres, assert regulatory control over platforms, and reduce dependency on Western or Chinese technology providers. However, in several countries, national DPI architecture remains deeply dependent on external financing, foreign technology providers, and international standards. Senegal's New Deal Technologique, South Africa's *MyMzansi* programme and Ethiopia's August 2026 creation of *Faydaverse* show stronger state ambitions to control national digital infrastructure. At the same time, the World Bank and other development partners, MOSIP, telecom operators, global payment networks and technology vendors remain central in the financing, procurement, development and operation of several DPI systems.

Rather than eliminating foreign influence, the rapid scale-up of DPI systems have now created new, deeply entrenched vectors of technological, financial and geopolitical dependence. The primary driver of this structural dependence is the crucial role played by multilateral development finance institutions and bilateral donors such as the World Bank, AFD, EIB, among others, as the dominant financiers and standard setters of African DPI across eight of the study countries. Simultaneously, state authorities face severe commercial vendor lock-in and long-term financial extraction by private technology contractors and system integrators, under multi-year public-private partnerships such as those with the Margins Group / Identity Management Systems (IMS) in Ghana, IDEMIA Smart Identity in Nigeria, Webmasters Limited in Kenya, Uqudo in Tunisia, Mulk International in Zimbabwe, and Tahaluf Al Emarat in Uganda. To counteract this, governments in Ethiopia and Uganda, for example, are adopting open source architectures such as MOSIP as an alternative pathway to autonomy.

Across Africa, ID and election procurement also show the practical limits of sovereignty where critical systems depend on proprietary devices, remote support, external hosting or supplier-controlled intellectual property. Rights-respecting sovereignty therefore also requires audit rights, data and key control, continuity planning, transparent subcontracting and the practical ability to change vendors without losing public records or service continuity.

Ultimately, digital sovereignty cannot be realised by political declarations, enacting data residency laws, or switching technology suppliers. The future of "digital sovereignty" can therefore move in two directions. On one hand, it can increase public capacity to set standards, retain data stewardship, develop local expertise, and reduce vendor lock-in. But on the other hand, it can also centralise more technical and informational power inside executive-controlled institutions without improving democratic accountability. This distinction is evident in *Faydaverse* and Project Pangolin, where state ownership or sovereign infrastructure is not, by itself, the same as independent oversight, citizen control or a right to remedy. A rights-respecting sovereignty agenda must combine national capability with transparent procurement, interoperable/open standards where appropriate, en-

forcing non-waivable vendor due diligence requirements, institutional separation, transparency, public scrutiny, and resisting donor-driven milestone pressure. Without robust structural conditions, state efforts to build DPI could continue to reproduce foreign technological dependence, leaving national DPI vulnerable to foreign commercial extraction, geopolitical leverage and unmonitored surveillance.

5.8 Looking Ahead and the Trajectories Shaping the Future

The direction of change is neither uniformly progressive nor uniformly regressive. Developments in the past three years have seen the strengthening of safeguards or access, while the principal risks have also become more systemic as identity, payments, connectivity, and data exchange are linked. The recent progressive developments are also notable. Continental policy frameworks became more specific between February 2024 and May 2025. Egypt moved a dormant data-protection framework into operation in November 2025. Courts in South Africa, Senegal, Ghana and Uganda issued significant rights decisions between January 2024 and March 2026. Ethiopia and Zambia reached their 2026 election periods without a detected shutdown. Also, several countries are retaining or expanding assisted and physical channels alongside digital services. These developments demonstrate that legal, institutional and design choices can alter the direction of DPI governance.

DPI is expanding state capacity and service reach across the study countries, but democratic and rights outcomes remain contingent on design choices. The most progressive direction combines practical inclusion gains with operational safeguards: alternative access, clear legal authority, transparent data sharing, independent regulators and courts, open connectivity during political competition, and remedies that are implemented. The principal challenge is that integration can make a single identity, data, or connectivity failure affect several rights at once. Technical maturity and accountability therefore need to be measured separately and improved together.

The challenges are also changing in character. Earlier debates focused heavily on whether people could enrol or whether a data-protection law existed. This next phase is increasingly about what happens after systems interconnect. The important questions shall be whether one error is propagated across agencies; whether data queries can be audited; whether private intermediaries remain accountable when they perform public functions; whether open connectivity survives political pressure; and whether a person can obtain a correction as quickly as a system can deny access. The policy objective is therefore not to slow useful digitalisation for its own sake, but to make safeguards operational at the same scale and speed as the infrastructure.

DPI is not producing a single democratic trajectory across Africa. It is increasing the capacity of states to identify, verify, connect and serve people. Whether that strengthens digital rights and democracy depends on who can access the systems, how visible citizens become to the state, whether networks remain open during political contestation, and whether independent institutions can constrain and remedy the misuse of digital public power.

If the patterns visible in 2026 continue, the most plausible continental future scenario is neither universal rights-respecting DPI nor uniform digital authoritarianism. It is a two-stage convergence in which identity, payments and data exchange become more interoperable while legal, regulatory and civic safeguards catch up unevenly. The actions by countries around law, institutional reform, design decisions, litigation, political transition and public pressure can change the direction of development of DPI.

Across Africa, the interaction of DPI, digital rights, and democratic governance is likely to evolve along four trajectories.³⁴⁵ First, identity and population registers will probably become more important as reusable eligibility services, including for elections. Second, hybrid electoral design is likely to persist because paper and offline mechanisms provide independent evidence and continuity even as front-end administration digitises. Third, AI and automated matching will move disputes from data collection toward inference, risk scoring and opaque decisions. Fourth, compute and power will determine the location of cloud regions, data centres and AI infrastructure, which are likely to concentrate in countries where fibre, electricity, demand and regulation are strongest.³⁴⁶ Given the cross-border dependencies, regional cooperation will therefore become important as data sovereignty. The rights-respecting trajectory combines selective interoperability, independent institutional mandates, open connectivity, public verifiability and rapid remedy. The higher-risk trajectory couples deeper linkage with weak civic space, common-mode

³⁴⁵ International IDEA. (2026, January 21). The case for a democracy stack: Rethinking digital public infrastructure for democratic societies. <https://www.idea.int/sites/default/files/2026-02/the-case-for-a-democracy-stack.pdf>; International IDEA. (2017, June 20). Introducing biometric technology in elections. <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>; African Commission on Human and Peoples' Rights. (2026, March 13). Resolution on elections in Africa in 2026 (ACHPR/Res.655 (LXXXVI) 2026). <https://achpr.au.int/index.php/en/adopted-resolutions/achprres655lxxxvi-2026>; African Union Commission. (2023, December 11). AU interoperability framework for digital ID. https://www.au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf

³⁴⁶ World Bank, Digital Progress and Trends Report 2023 <https://www.worldbank.org/en/publication/digital-progress-and-trends-report>; International Energy Agency, Data Centres and Data Transmission Networks <https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks>

failures and executive visibility across services and political participation.

Kenya suggests a further continental trajectory, where rights disputes may migrate from visible enrolment systems to less visible interoperability layers. Between the 2019–2024 litigation over NIIMS and Maisha Namba³⁴⁷ and with the 2024–2026 expansion of APIs, digital-health exchange and national data-governance planning, there is a shift from whether the state may collect a person's identity data to how many systems may reuse it and under what conditions. If this pattern spreads, future digital-rights oversight will require technical capacity to inspect API permissions, access logs, data provenance, automated decisions, and cross-system correction, not only legal rules governing the original database.

Three distinct continental pathways could emerge. Firstly, a rights-respecting integration is possible. Reusable identity could lower documentation burdens; interoperable payments could improve social transfers and public revenue; data exchange could reduce repeated collection; open-source architecture could reduce vendor lock-in; independent authorities could strengthen oversight; and digital systems could strengthen verification and public access to services. For this path to hold, governments would need to preserve workable offline alternatives, publish pre-deployment impact assessments and data-sharing rules, fund independent regulators, make correction portable across services, keep communications open during political competition and implement court and regulatory remedies rather than merely acknowledge them. This pathway fosters high public trust, resilience service delivery and enforceable judicial remedy.

A second path is a mixed system of high service capacity and uneven rights protection. Technical benefits are likely to continue to expand with rapid scaling up of DPI, especially for already formally documented and connected urban users, while exclusion, surveillance and remedy problems become concentrated among traditionally marginalised and digitally excluded groups least able to challenge them. This could produce stratified digital citizenship in which the state becomes easier to deal with for some people and harder to correct for others. Formal laws could exist on paper, but executive subordinated regulators fail to enforce rules against public sector entities. The democratic risk would be less a single dramatic abuse but the normalisation of opaque eligibility decisions, cross-system profiling and lengthy correction processes as routine features of administration. This pathway could create cascading exclusion for vulnerable populations, unaddressed biometric errors and persistent lock in.

A third, more concerning path is a securitised and authoritarian approach where civic space and institutional independence deteriorate while technical integration deepens. In such settings, identity, connectivity, payments and data exchange are integrated in state intelligence and surveillance apparatus and can make restrictions on expression, association, movement or economic participation more targeted and more difficult to contest. Election-period internet disruptions, surveillance concerns, repressive laws and broad security powers and their chilling effects in parts of the study countries show that this risk is not hypothetical, although technical capability should not be equated with political intent. The decisive variables are lawful purpose, independent authorisation, transparency, contestability and effective remedy.

Several near-term developments will show which path is taking hold. Kenya and Nigeria's upcoming 2027 general elections will test the legal requirement for electronic transmission of polling-unit results and its paper fallback.³⁴⁸ South Africa's Digital ID and *MzansiXchange* will test whether a comparatively strong rights framework remains effective as interoperability moves from pilot to scale. Tunisia will show whether sector-specific mandatory Mobile ID expands while credible alternatives remain available. Zimbabwe's 2026–2030 Project Pangolin roadmap and Ethiopia's *Faydaverse* model will test whether sovereignty and state capacity are matched by independent governance. Ghana and Senegal will test whether developing data-exchange layers can carry forward the accountability gains visible in recent court decisions.

The overall implication is that the future rights impact of DPI will be determined during this period of transition, not after DPI systems are fully entrenched. The window for embedding democratic and rights-respecting DPI is widest now before mandatory dependencies multiply. In the coming years, the most important distinction may therefore be between countries that treated human rights and democratic safeguards as part of DPI design and those that treated them as compliance measures added after technical integration.

347 Kenyalaw. (2024, August 12). *Haki na Sheria Initiative v. Attorney General & 4 others* [2024] KEHC 10021 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2024/10021/eng@2024-08-12>; High Court of Kenya. (2020, January 30). *Nubian Rights Forum & 2 others v. Attorney General & 6 others; Child Welfare Society & 8 others (Interested Parties) (Petition 56, 58 & 59 of 2019, Consolidated)* [2020] KEHC 8772 (KLR). <https://new.kenyalaw.org/akn/ke/judgement/kehc/2020/8772>; MyGov, Kenya. (2024, November 13). KRA launches 'GavaConnect' API to modernize tax administration and spur innovation. <https://gaa.go.ke/kra-launches-gava-connect-api-modernize-tax-administration-and-spur-innovation>; Ministry of Information, Communications and the Digital Economy, Kenya. (2026, February 6). Government moves to strengthen Kenya's data governance framework. <https://ict.go.ke/government-moves-strengthen-kenyas-data-governance-framework>

348 National Assembly of Nigeria. (2026, February 18). Electoral Act, 2026 (Act No. 1). ss 60 <https://nass.gov.ng/documents/download/11248>; Independent National Electoral Commission, Nigeria. (n.d.). Upcoming elections. Retrieved September 13, 2026, from <https://www.inecnigeria.org/upcoming-elections/>

6.0 Conclusion and Recommendations

6.1 Conclusion

Digital Public Infrastructure is rapidly expanding across Africa. It is effectively galvanising interoperable identity, payment, and data-exchange systems, which is equally playing a critical role in shaping the relationship between states and citizens through the opportunities it presents in effective administrative efficiency and financial inclusion. However, these systems are not purely neutral in operations. They have overarching effects on design and governance on the continent. Foundational credentials such as mandatory gateways and access to essential public and private services are increasingly facing flaws in architectural design and utility, technical failures, and inaccurate records. The effect is often a trigger of widespread, cascading exclusion for vulnerable populations, particularly those facing barriers in digital literacy, connectivity, or civil registration, such as rural dwellers, women, children and the elderly.

While institutional progress is quite visible on the continent with progressive judicial interventions and regulatory enforcement in recent times such as Ghana, Senegal, South Africa, and Uganda, the legal and technical capacities are largely lacking and uneven. Technical integration is progressing much faster than institutional frameworks which are required for effective governance. The effect, as shown in the study findings, is fragmented oversight, opaque and poor data-sharing practices, and limited public verifiability. Furthermore, the convergence of foundational identity systems with the work of EMBs and democratic processes and the telecommunications infrastructure has exposed citizens to severe democratic risks, where network disruptions and administrative flaws lead to impairment of political participation and the protection and enjoyment of civic freedoms.

Ultimately, the legitimacy and trust of African DPI largely depend on the establishment and integration of robust, rights-respecting safeguards into the system functioning rather than treating them as retroactive compliance measures. Ensuring a resilient, functional and inclusive digital future requires maintaining accessible non-digital channels, enforcing data protection principles and rights with strictness placed on purpose and data minimisation, ensuring independent institutional oversight, ensuring open connectivity in democratic seasons and political transitions, and providing timely, fair enforceable avenues for access to legal remedy.

6.2 Recommendations

This report has examined how Digital Public Infrastructure (DPI) systems are reshaping the relationship between states and citizens, particularly regarding digital rights, democratic governance, and civic participation across eleven African countries: Egypt, Ethiopia, Ghana, Kenya, Nigeria, Senegal, South Africa, Tunisia, Uganda, Zambia and Zimbabwe. The application of DPI is however still underdeveloped, with flaws in transparency and governance. This requires both intentional and calculated efforts by different stakeholders, including governments, regional bodies, private sector civil society, media, and academia to ensure successful and effective deployment and utility of DPI systems. Below are some of the recommendations which, if rightly implemented, will potentially contribute to efficient DPI infrastructure and systems on the continent.

6.2.1 Governments and Public Institutions

Given that governments are expanding identity, interoperability and digital-service mandates, the priority should be to make rights safeguards and alternatives part of the same DPI design and implementation life cycle.

- Establish robust governance, including rights-respecting national policies, laws, strategies and action plans to drive DPI adoption and investment in the complementary infrastructure to foster connectivity, innovation, and capacity enhancement.
- Keep essential public services accessible through assisted, in-person or otherwise non-digital channels wherever identity, connectivity, disability, literacy, or device access can create exclusion. Digital-first should not become digital-only for survival services.
- Mandatorily rR Human mandatory hmpactrAssestidn Impact Assesslmpaet Assessment b assessments identity, bioDPI digital or deployed or significantly expanded, with particular attention to exclusion, discrimination, surveillance, cybersecurity, function creep and access to remedy.entre and cable investment as a shared, coordinated regional asset and also map and publish each major DPI system's critical dependencies.
- Replace coverage-only targets with disaggregated meaningful-connectivity and service-completion indicators.
- Build a single, accessible correction pathway for foundational identity errors that propagates verified corrections to connected services, rather than requiring citizens to repair the same record across multiple agencies.
- Publish data-sharing rules, system purposes, categories of authorised users, retention periods, procurement information, and audit arrangements in language accessible to the public.
- For each major DPI programme, maintain a public implementation record stating the responsible agency, legal basis, launch or pilot date, current operational status, mandatory-use rules, key suppliers/financiers, categories of users affected, published audit/impact-assessment status, and available correction or complaint routes.
- Stop internet shutdowns and other blanket connectivity restrictions as tools of political or security management, including before, during and after elections, in line with ACHPR Resolutions 580 (2024) and 655 (2026).
- Where national identity, civil-registration or population data are used for voter registration, voter identification or voter-register maintenance, preserve electoral-management-body custody and decision-making authority; use minimum-attribute, logged verification where possible; provide lawful alternative verification and

rapid correction; and ensure that identity-system errors do not become disenfranchisement.

- Require electoral law and operational procedures to specify tested manual/offline fallback for registration and polling, the status of paper records relative to electronic outputs, incident escalation, extension of voting where necessary, and preservation of evidence for challenge. Fallback should be treated as a rights safeguard, not an informal workaround.
- Require independent testing, stress testing, certification where appropriate, auditability, and proportionate public disclosure of election technologies that rely on foundational identity, shared government data, or results transmission. Parties, observers, and oversight bodies should have meaningful access to the evidence needed to assess operation without compromising ballot secrecy, system security, or personal data.
- For high-impact automated or AI-assisted electoral or DPI systems, require a public register of use cases, a clear legal basis, recurring HRIA/DPIA/EQIA, data and model provenance, bias and accessibility testing, human review, incident reporting, and a route to contest an automated outcome.
- Separate or strictly govern high-risk access to identity and service data by law-enforcement and national-security bodies through necessity, proportionality, independent authorisation, access logging, and post-hoc oversight.

6.2.3 Data Protection Authorities, Sector Regulators, and Oversight Institutions

Formal oversight powers are becoming more common, but DPI-specific enforcement, cross-regulator coordination, and public reporting remain uneven.

- Prioritise proactive audits of national identity databases, interoperability platforms, and government-to-person payment systems rather than relying only on complaints after harm occurs.
- Publish enforcement statistics and outcomes in a form that distinguishes public-sector, foundational-ID and cross-system data-sharing cases from ordinary private-sector compliance.
- Develop joint supervisory protocols for cases that cross identity, telecoms, finance and e-government systems, so that fragmented mandates do not produce accountability gaps.
- Where election systems query foundational identity or population data, agree on a supervisory protocol between the electoral authority and the relevant data-protection or identity regulator covering lawful attributes, controller responsibilities, security, logs, correction, retention, incident response, and independent audit, without compromising EMB independence.

- Telecommunications and infrastructure regulators should publish granular affordability, technology-generation, quality, outage, restoration, wholesale-access, and universal-service-fund data. Oversight should verify that route, hosting, and power redundancy is genuine and does not share physical or contractual points of failure.
- Create accessible complaint channels that work for people with low literacy, limited connectivity, disability, or no digital credential, as they are the groups most likely to experience exclusion.
- Protect institutional independence through transparent appointments, secure budgets and powers to investigate public bodies without executive permission.

6.2.4 Private Technology Providers, Telecom Operators, Banks, and Payment Firms

Private intermediaries perform more public-facing DPI functions than their public human-rights accountability currently reflects.

- Conduct and publish UNGP-aligned human-rights due diligence for high-risk public-sector identity, biometric, data-exchange and surveillance contracts, including risks created by downstream government use.
- Treat frontline service points and private intermediaries performing public functions as accountable components of DPI, with clear service standards, correction obligations and escalation routes.
- Adopt privacy and security by design, data minimisation, clear purpose limitation and robust access logging; prohibit secondary use of public-system data without a lawful basis and transparent safeguards.
- Provide contractual transparency sufficient for public oversight of critical public infrastructure, while protecting legitimately confidential security information.
- For DPI, election and other high-stakes public technology contracts, require enforceable rights to system and security logs, audit and testing, data portability and ownership clarity, source-code review or escrow where appropriate, continuity support, incident disclosure, subcontractor transparency, termination assistance, and timely remediation. Procurement should make UNGP-aligned human-rights due diligence a performance obligation rather than a voluntary statement.
- Extend UNGP-aligned due diligence across network controls, land, construction and worker safety, energy and water use, supply chains, outage handling, restriction orders, and responsible exit. Telecom, cloud and data-centre firms should disclose salient impacts, critical dependencies, and corrective action, and provide or cooperate in remedy.

6.2.5 Development Partners and DPI Financiers

External finance and technical assistance increasingly influence architecture, scale and milestones. Rights, remedy and institutional independence should also be measured with equal specificity.

- Link disbursement and scale milestones to verified inclusion, oversight, and remedy outcomes and not only registration totals, platform launches, or transaction volumes.
- Avoid financing electoral or DPI integration on the assumption that shared identity is inherently more efficient. Support pilots that measure exclusion, false matches, correction time, accessibility, resilience, and institutional independence before a foundational credential becomes the sole route to a political right, or essential service.
- Fund independent technical, human-rights, and accessibility audits that are published before mandatory-use rules are expanded.
- Support the long-term capacity and independence of domestic regulators, courts, civil society, and complaint systems rather than building project-specific safeguards that disappear when financing ends.
- Require vendors and implementing partners to disclose human-rights due diligence and remedy arrangements as part of procurement and programme supervision.
- Finance open-access, route-diverse, energy- and climate-resilient infrastructure alongside DPI. Milestones should measure affordable use, service completion, outage recovery, local operational capability, and supplier exit readiness, rather than fibre, coverage, enrolment or transaction volume alone.

6.2.6 Civil Society, Media, and Academia

Civil society has been most effective through litigation, investigation, and post-harm advocacy. The next step is stronger participation before procurement and rollout.

- Move DPI scrutiny upstream by engaging in policy, procurement and impact-assessment processes before systems are launched, while retaining strategic litigation where necessary.
- Document lived experience of identity errors, authentication failure, exclusion, surveillance and remedy using disaggregated evidence on gender, disability, age, income, geography, migration, and citizenship status.
- Investigate data-sharing arrangements, vendor relationships, and public procurement as democratic-governance issues, not only as technical matters.
- Document technology-facilitated gender-based violence and other information-environment harms that deter women and marginalised groups from political participation, while distinguishing these harms from DPI-specific causation. Use ACHPR Resolution 522 as a regional accountability benchmark.
- Build civil-society and media capacity to scrutinise less visible infrastructure: identity-to-election APIs, access logs, vendor and hosting arrangements, automated matching, recommender systems and AI-assisted election tools.
- Build public literacy around both the benefits and the rights implications of DPI, including how to access, correct, and challenge data held by public institutions.

6.2.7 Regional Economic Communities, and Regional Courts

Continental and regional norms are becoming stronger, but ratification, implementation, and enforceable remedies remain uneven across regions.

- Use the African Charter, the Malabo Convention, the AU Data Policy Framework, the African Digital Compact, the AfCFTA Protocol on Digital Trade, and the Universal DPI Safeguards Framework to develop minimum rights-respecting DPI standards. The priority is both wider participation and demonstrable domestic implementation.
- Create regular continental reporting on identity exclusion, DPI-related complaints, high-risk public-sector data processing, election-period internet restrictions, and cross-border data-sharing practices.
- Operationalise ACHPR Resolution 580 (2024) together with Resolution 655 (2026) through systematic election observation, public reporting, and follow-up when states order shutdowns or platform restrictions; incorporate assessment of EMB independence, digital violence, disinformation responses, and access to effective redress.
- Develop regional resilience standards and cross-border restoration protocols for infrastructure carrying DPI, including outage reporting, open-access corridors, and continuity arrangements for landlocked states. Promote portable workloads, open standards, and shared technical capacity so national systems do not depend on the same small supplier set.
- Develop regional guidance for election-related use of foundational digital identity, building on the AU Interoperability Framework for Digital ID. The guidance should favour selective disclosure and minimum-attribute verification, protect electoral-register independence, require auditable correction and fallback, and prohibit non-electoral surveillance through electoral data connections.
- Build on the ECOWAS Court's Senegal precedent by making regional digital-rights remedy more accessible and by supporting domestic implementation of judgements.
- Promote interoperability standards that include governance interoperability such as compatible rules for audit, correction, consent where appropriate, lawful access and remedy, rather than focusing only on technical exchange.



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

☎ +256 414 289 502

✉ programmes@cipesa.org

✕ @cipesaug 📘 facebook.com/cipesaug 🌐 LinkedIn/cipesa

🌐 www.cipesa.org