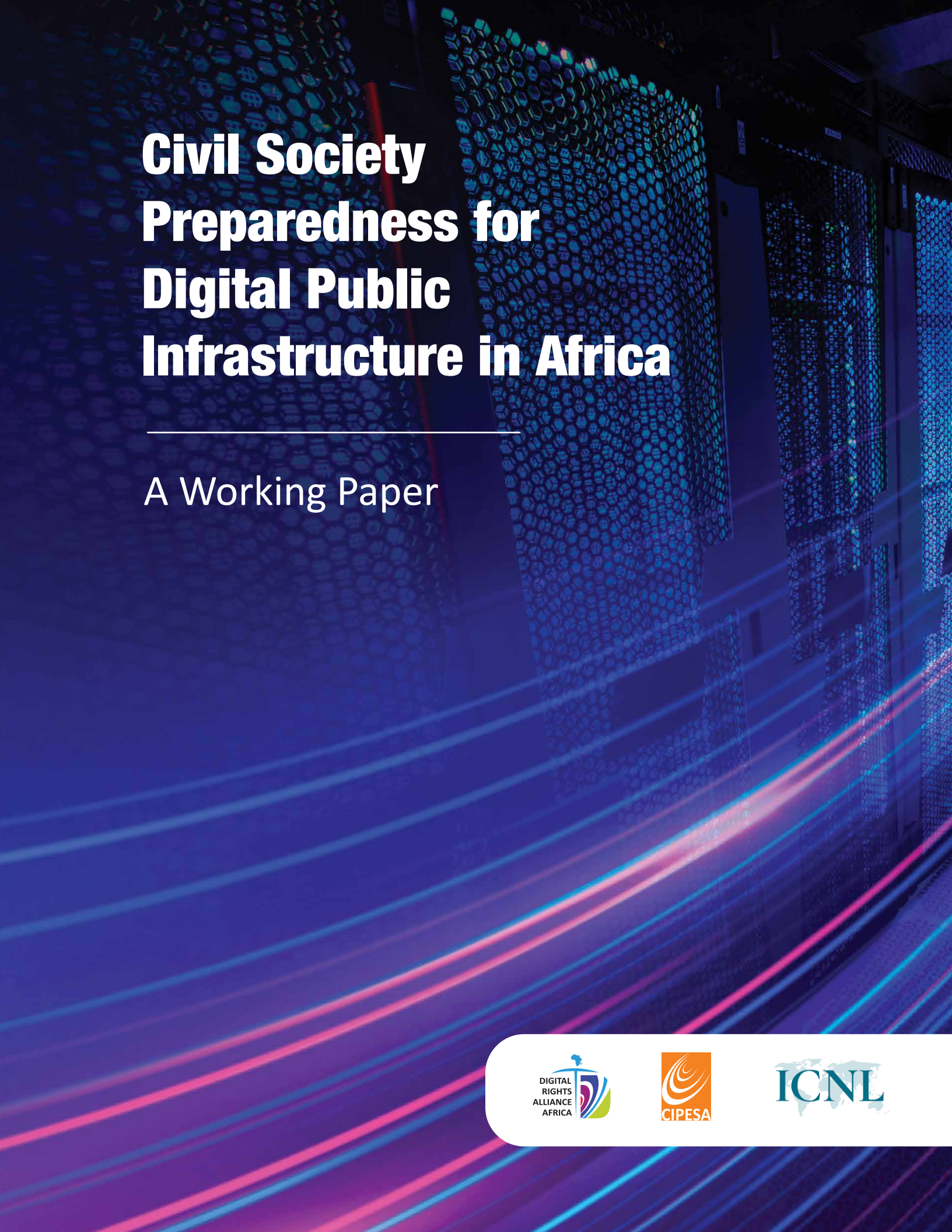


Civil Society Preparedness for Digital Public Infrastructure in Africa

A Working Paper

DIGITAL RIGHTS ALLIANCE AFRICA

CIPESA

ICNL

Table of Contents

List of Abbreviations

DPI:	Digital Public Infrastructure
ID:	Identity
CSOs:	Civil Society Organisations
NGO:	Non-Governmental Organisation
ACHPR:	African Commission on Human and Peoples' Rights
NIRA:	National Identification and Registration Authority
HRIA:	Human Rights Impact Assessment
NHRIs:	National Human Rights Institutions
ICT:	Information and Communication Technology
DPAs:	Data Protection Authorities
DA4TI:	Digital Agenda for Tanzania Initiative
UNDP:	United Nations Development Programme

Executive Summary

Digital Public Infrastructure (DPI) is a network of technical systems that forms the backbone of the digital state.[1] It shapes how citizens are recognised by governments, access essential services, participate in democratic processes, and exercise fundamental rights.[2] DPI spans multiple sectors, including identity, finance, health, education, governance, and civic participation, and includes systems such as digital identity platforms, interoperable government databases, and citizen engagement tools. Its capacities determine visibility, participation and empowerment of those involved. DPI is therefore a technical foundation and a civic instrument that defines the contours of participation, inclusion and rights in the digital era.

Current decisions about the design, governance, and deployment of DPI will resonate for generations, setting the digital contract between citizens and the state. Poorly designed systems risk exclusion, abuse, and expansion of undue surveillance. On the other hand, well-governed, rights-respecting DPI systems can expand civic space, enhance democratic participation, and protect rights such as privacy. Like the rest of the world, in Africa, these systems are also being designed and deployed, but often with limited public scrutiny. For civil society, the stakes are profound considering the implication it has on democratic governance, rights and public oversight.

In this context, the role of Civil Society Organisations (CSOs) and their preparedness for DPI is essential. They cannot afford to be passive observers, but must lead, engage, and safeguard DPI from the outset. This approach and role entails upstream engagement; monitoring and accountability; public education and awareness; capacity building; and regional collaboration. This paper outlines warning signs, human rights frameworks, and strategic tools and action for CSOs to proactively influence DPI governance to ensure that DPI systems serve citizens, protect rights, and strengthen democratic participation, instead of consolidating power or excluding vulnerable and marginalised communities. Thus, civil society's engagement, expertise, and vigilance are imperative for democratic empowerment and inclusion, and to counter potential control, exclusion, and surveillance risks.

1 https://www.undp.org/digital/digital-public-infrastructure (accessed 2 May 2026).

2 See for instance: UNDP: Driving Digital Transformation In Somalia: 2025 Highlights https://undpsomalia.exposure.co/promoting-innovation-and-digital-transformation-in-somalia 9 April 2026 (accessed 2 May 2026).

1. What is Digital Public Infrastructure?

DPI refers to the foundational digital systems that enable governments, businesses, and citizens to interact and transact in the digital environment. [3] Increasingly described as the backbone of the digital state, DPI provides the shared digital rails upon which public services, social protection systems, financial transactions, and civic participation mechanisms operate.[4] While often framed in technical terms, DPI is not only a collection of service delivery tools, instead, it constitutes a governance infrastructure that shapes how individuals are recognised by the state, how they access essential services, and how they exercise rights and participate in public life.[5]

Typically, DPI includes a set of interoperable systems such as digital identity platforms, digital payment infrastructures, and data exchange frameworks that enable different government agencies and service providers to interact seamlessly.[6] These components allow governments to authenticate identities, deliver social benefits, process financial transactions, and integrate data across sectors such as health, education, taxation, and social protection. When effectively governed, such systems can improve efficiency, expand financial inclusion, and enhance access to services, particularly for populations historically excluded from formal systems.[7]

The significance of DPI extends beyond administrative efficiency. These systems determine who is recognised, authenticated, and able to interact with government services, and they also directly influence citizenship, participation, and access to rights.[8] A digital identity system, for instance, may determine whether individuals can open a bank account, receive social protection benefits, register a business, or vote. Interoperable government databases may improve service coordination, but they can also enable large-scale data aggregation that raises concerns about surveillance, privacy, and data protection.[9] For these reasons, DPI then functions as the architecture of the digital state.

3 *United Nations Development Programme (UNDP): 'Digital Public Infrastructure (DPI)'https://www.undp.org/digital/digital-public-infrastructure?gad_source=1&gclid=Cj0KCQjw3vO3BhCqARIsAEWbIcC6eX8iuQeMsPLsYCmpTQMevf1ma0KYl3rplZUsL9qUWI1KGvqnGBIaAhLSEALw_wcB (accessed 2 May 2026).*

4 *UNDP: https://www.undp.org/digital/digital-public-infrastructure (accessed 2 May 2026).*

5 *World Bank: 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 (accessed 2 May 2026).*

6 *United Nations University: Z Jordanoski. 'Safeguarding Digital Public Infrastructure: A Global Imperative for Sustainable Development' 9 July 2025 https://unu.edu/egov/article/safeguarding-digital-public-infrastructure-global-imperative-sustainable-development (accessed 2 May 2026).*

7 *As above.*

8 *See DigID: 'Doing Digital Identities' https://cordis.europa.eu/project/id/101039758/reporting (accessed 2 May 2026).*

9 *S de Carvalho Homem "From Innovation to Inclusion? The Human Rights Dilemma of Digital Citizenship" (2026) https://www.shs-conferences.org/articles/shsconf/abs/2026/03/shsconf_ichss2026_01001/shsconf_ichss2026_01001.html (accessed 2 May 2026).*

2. Core Components of DPI

Digital Identity (ID) Systems

National identity frameworks that verify citizens' identity, forming the gateway to public services, social protection programmes, voting registration, and financial inclusion. By enabling recognition and authentication, digital IDs are central to civic participation, but they also carry risks of exclusion if access is uneven or safeguards are weak.

National ID databases, biometric registration systems like India's Aadhaar (inclusive service access)[10], Kenya's Huduma Namba [11] (risk of exclusion and surveillance critiques).

Digital Payment Platforms

Infrastructure enabling government-to-person transfers, tax collection, subsidy disbursement, and other financial flows. They operationalise social protection and service delivery, making state benefits and obligations accessible in real-time. The integrity, transparency, and privacy of these platforms directly impact citizens' trust in state systems.

Government-to-person cash transfer systems, [12] tax payment portals, [13] and subsidy disbursement platforms.[14]

Data Exchange Platforms

Interconnected systems that facilitate secure, lawful, and interoperable data sharing across sectors such as health, education, and social protection. These platforms enable holistic service delivery and policy integration but raise critical questions about data governance, privacy, and rights-respecting interoperability.

Health information exchanges,[15] integrated education-management databases,[16] and cross-sector social protection platforms.[17]

Interoperable Government Databases

Technical and policy frameworks allowing different government agencies to share data and deliver services seamlessly. Interoperability reduces administrative friction, enhances efficiency, and supports evidence-based policymaking. However, without robust safeguards, these databases can create powerful tools for surveillance or exclusion.

Multi-agency citizen service portals, e-government platforms integrating welfare, taxation, and licensing services.[18]

10 https://uidai.gov.in/en/ (accessed 3 May 2026).

11 Government of Kenya: https://www.hudumakenya.go.ke/ (accessed 3 May 2026).

12 For instance, Togo's Novissi platform which was originally launched as an emergency COVID-19 response, has since been institutionalised as a permanent national social protection programme, delivers cash transfers to vulnerable households via mobile money. See here: C Cheney 'Why donors are backing a global push for digital public infrastructure' 30 September 2022 https://www.devex.com/news/why-donors-are-backing-a-global-push-for-digital-public-infrastructure-104007?ref=balance.commonedge.asia (accessed 3 May 2026).

13 For example, Nigeria's Merchant Buyer Solution (MBS) e-Invoicing platform is a digital tax compliance system. It was implemented by the Federal Inland Revenue Service (FIRS), and standardises invoice creation and exchange across public and private sectors using a pre-clearance model where invoices must be validated in real time before reaching buyers. It represents a strategic shift from manual filings to digital, transaction-level tax oversight. See B Joseph 'Nigerian Government Launches E-Invoicing Platform to Enhance Tax Transparency and Boost Revenue Efficiency' 2 May 2025.https://msmeafricaonline.com/nigerian-government-launches-e-invoicing-platform-to-enhance-tax-transparency-and-boost-revenue-efficiency/ (accessed 3 May 2026).

14 An example of this is the Rwanda Smart Nkunganire System (SNS) is a digital agricultural subsidy platform that has revolutionised the delivery of fertilizers and seeds to smallholder farmers. It was developed through a public-private partnership between BK Techouse and the Rwanda Agriculture and Animal Resources Development Board (RAB), the SNS digitizes the agricultural input supply chain by creating a centralized stakeholder database, monitoring input demand and supply at all levels, and enabling cashless subsidy transactions. See CGIAR: Assessing Delivery and Business Models for High Impact Digital Solutions at Scale: The case of Rwanda Smart Nkunganire System (SNS), October 2024 https://cgspace.cgiar.org/server/api/core/bitstreams/a9de32d9-7152-48c0-b064-d3990526d006/content (accessed 3 May 2026).

15 For instance, the Rwanda National Health Intelligence Centre (NHIC) is a centralised platform for processing, integrating, triangulating, and analyzing real-time health data using advanced technological tools and artificial intelligence. It serves as a strategic hub for evidence-based decision-making and policy development, drawing data from community health workers, health posts, health centers, district and referral hospitals together with other domains including disease prevention and surveillance, emergency response, health workforce, health financing, supply chain management, and civil registration and vital statistics. See Government of Rwanda: National Health Intelligence Center (NHIC) https://www.moh.gov.rw/sites-apps/nhic (accessed 3 May 2026).

16 An example of this is The Gambia's Education Management Information System (EMIS), which is built on the open-source DHIS2 platform. It represents a significant shift from static, paper-based annual reports to dynamic, learner-centered data management. See Ministry of Basic and Secondary Education (MoBSE), The Gambia. (2026). 'The Gambia charts a path to data-driven education with DHIS2'. https://education.dhis2org/gambia-data-driven-education/ (accessed 3 May 2026).

17 An example of this is Ghana's Single Window Citizens Engagement Service (SWCES), a centralized digital platform for social protection grievance redress and information sharing, operational since 2017. See Ministry of Gender, Children and Social Protection (MoGCSP), Ghana. (n.d.). Single Window Citizen Engagement Service (SWCES). https://www.mogcsp.gov.gh/projects/swces/(accessed 3 May 2026).

18 Several governments in Africa have launched multi-agency citizen service portals that converge multiple services onto unified Digital Public Infrastructure platforms. Notable examples include Kenya's e-Citizen platform (offering over 21,000 services to more than 13 million users), Ethiopia's MESOB(integrating 12 federal institutions providing 41 services via an API gateway), Rwanda's Mbaza platform (enabling AI-powered citizen feedback integrated with the Irembo e-governance portal), Nigeria's Government Service Portal (GSP) (connecting 12 pilot agencies including NIMC and Immigration Services), and Tanzania's Government Enterprise Service Bus (GovESB) (establishing interoperable data sharing across the digital identity authority, police, tax, and immigration services). See for instance: Government of Ethiopia: MESOB Centre https://mesobcenter.et/ (accessed 3 May 2026).

3. The Case for Civil Society Engagement

3.1 DPI as Constitutional and Civic Infrastructure

Beyond being a technical infrastructure, DPI shapes the constitutional contours of citizenship in the digital age. When identity systems, public services, financial transactions, and administrative records are digitised, DPI becomes an invisible architecture that structures state–citizen relations. Decisions about how these systems are designed, governed, and regulated have implications for inclusion, participation, and democratic accountability.

3.1.1 Who is Visible to the State?

In many countries, digital identity systems are the gateway through which individuals are recognised by public institutions. Citizens who lack digital identification, reliable connectivity, or digital literacy may find themselves excluded from formal recognition, which can limit access to essential services, social protection, public participation and other legal rights more broadly. In the absence of safeguards for inclusion and accessibility, digitisation risks deepening existing inequalities by marginalising individuals who already face barriers related to geography, poverty, disability, documentation, gender, age, language, literacy, connectivity, infrastructure and statelessness.[19]

3.1.2 Who Can Access Essential Services?

Increasingly, access to healthcare, education services, financial systems, and social protection programmes is mediated through digital platforms that rely on digital identification, data interoperability, and electronic payment systems. While these systems can significantly improve efficiency and reduce administrative burdens, they also create new dependencies on digital infrastructure. When systems fail, when authentication mechanisms are unreliable, or when individuals lack the necessary digital credentials, access to services can be interrupted, denied,[20] or even death in extreme circumstances. In documented cases, individuals have been locked out from accessing healthcare or their pensions because their fingerprints could not be read, their phones lost network signal, or their digital identity systems crashed for months at a time.[21] In the most extreme failures, living people have been erroneously declared dead in government databases, rendering them entirely invisible to service providers and unable to access banking, medical treatment, or social benefits.[22]

19 *Policy Brief: Utilising Digital Public Infrastructures for Social Protection in G20 Countries https://t20southafrica.org/publications/utilising-digital-public-infrastructures-for-social-protection/#elementor-action%3Aaction%3Dpopup%3Aopen%26settings%3DeyJpZCI6IjEwMDciLCJ0b2dnbGUiOmZhbHNlfQ%3D%3D (accessed 3 May 2026).*

20 *See European Research Council: DigID - Doing Digital Identities https://cordis.europa.eu/project/id/101039758/reporting (accessed 3 May 2026).*

21 *'Broken system: How Kenya's digital health revolution is failing on the frontline', 9 December 2025 Daily Nation https://nation.africa/kenya/health/broken-system-how-kenya-s-digital-health-revolution-is-failing-on-the-frontline-5291546. (accessed 3 May 2026).*

22 *See also 'Rajasthan's elderly are victims of 'digital murder'. eKYC gaps leave lakhs without pension' 8 November 2024* **The Print** *https://theprint.in/ground-reports/rajasthans-elderly-are-victims-of-digital-murder-ekyc-gaps-leave-lakhs-without-pension/2347032/?utm_source=TPWeb&utm_medium=Telegram&utm_campaign=TappChannel. This is also illustrated in the Indian case of In Madhya Pradesh, a six-month-pregnant woman who was erroneously declared dead in government records, which blocked her Aadhaar and led to the denial of medical treatment, bank access, and government benefits. Local officials reportedly mocked her family and asked them to 'prove she was alive,' while correcting the error required higher-level approval and took 15 days, which put a risk on her pregnancy. . This case illustrates a catastrophic but not isolated failure mode when digital identity systems mark living people as dead, they become invisible to service providers, unable to access healthcare, banking, or social protection. See 'Six-Month Pregnant Woman Declared 'Dead' in Government Records, Denied Treatment in MP's Khajuraho' 13 January 2026 Dainik Jagran https://english.dainikjagranmpcg.com/states/madhya-pradesh/six-month-pregnant-woman-declared-%E2%80%98dead%E2%80%99-in-government-records-denied-treatment/article-12302 (accessed 5 May 2026).*

Uganda's national biometric ID system illustrates the promises and dangers of DPI. Following a revealing 2021 report that documented how the system had excluded 23–33 percent of adults from healthcare and social services, including an 80-year-old man who died traveling to a fingerprint verification site,[23] the government launched a digital ID renewal campaign between 2024 and 2026.[24] The new system successfully migrated nearly 29 million records onto an upgraded platform and introduced iris recognition technology to address the problem of unreadable fingerprints that had disproportionately excluded elderly people and manual labourers.[25] On paper, these were significant technical improvements. However, as of 2026, the core problem has not been resolved: a recent lawsuit alleges that up to one-third of Ugandan adults still lack the biometric ID card, and marginalised groups, particularly persons with disabilities, report being left behind despite government assurances of inclusion.[26] Moreover, new problems have emerged, including weak data protection enforcement. A January 2026 report by Unwanted Witness documented widespread privacy violations during Uganda's 2026 elections.[27] The key findings highlighted that:

- Voters received unsolicited political SMS, WhatsApp, and call messages without prior consent;
- Thousands were added to political WhatsApp groups without consent, exposing their phone numbers to strangers; and
- The Electoral Commission, a major holder of sensitive biometric data, was not registered with the Personal Data Protection Office and had no public privacy policy.

Uganda's trajectory shows that technological upgrades alone cannot fix DPI failures. Without sustained attention to governance, inclusion, and accountability, even the most sophisticated identity systems can reproduce the very exclusions they promise to solve. Digital identity failures can have lethal consequences.

3.1.3 Who can Participate in Democratic Life

Civic engagement, including voter registration, participation in public consultations, and communication with government institutions, is facilitated through digital platforms as part of national digital transformation strategies. In some contexts, digital systems support participatory governance by enabling citizens to provide feedback on public policy or engage in deliberative processes online. However, where such platforms are poorly designed, exclusionary, or subject to political control, they may limit meaningful participation and undermine the enjoyment of human rights and trust in democratic institutions. [28]

23 *Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, & 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' 8 June 202 15 https://drive.google.com/file/d/1EOgwFPMK_8TY_qUhWAASMk_b4f3HgRM3/view (accessed 5 May 2026).*

24 *DK Ssembuya 'Mass National ID Enrollment, Renewal for May 27' 6 May 2025 https://ugandaradionetwork.net/story/mass-national-id-enrollment-renewal-for-may-27 (accessed 5 May 2026).*

25 *Government of Uganda: 'Everything You Need to Know About Uganda's Mass National ID Renewal Exercise' 9 May 2025 https://govinfohub.go.ug/index.php/2025/05/09/everything-you-need-to-know-about-ugandas-mass-national-id-renewal-exercise/ (accessed 5 May 2026).*

26 *'Are disabled Ugandans being left out of digital ID system?' 17 February 2026 The Independent https://www.independent.co.ug/are-disabled-ugandans-being-left-out-of-digital-id-system/ (accessed 5 May 2026).*

27 *Unwanted Witness: 'Why Data Privacy Is the Missing Piece of Electoral Integrity' 27 January 2026 https://www.unwantedwitness.org/why-data-privacy-is-the-missing-piece-of-electoral-integrity/ (accessed 5 May 2026).*

28 *Institute of Development Studies: 'Africa's biometric-ID systems blocking millions of citizens from fundamental rights and services' 4 December 2025 https://www.ids.ac.uk/press-releases/africas-biometric-id-systems-blocking-millions-of-citizens-from-fundamental-rights-and-services/. See also C Firtin et al. 'Digital accountability through e-participation: the moderating role of the digital divide' Public Money & Management (2025) https://www.tandfonline.com/doi/full/10.1080/09540962.2025.2573784#d1e180 (accessed 6 May 2026).*

3.1.4 Who can Organise and Exercise Human Rights

The ability of civil society organisations (CSOs), journalists, and citizen groups to mobilise, communicate, and advocate for change is increasingly shaped by the digital systems that mediate public discourse. Platforms used for civic engagement, digital identification requirements for accessing services, and data governance frameworks can either enable collective action and transparency or create conditions that discourage dissent or restrict civic space.[29] Civil society actors are a particularly high-risk group because of their work, including, monitoring state accountability, advocating for marginalised communities, and mobilising political dissent. This role places them directly in the crosshairs of surveillance infrastructure. Digital ID systems restrict civil society in two ways: (i) by creating a surveillance apparatus that tracks activists' communications and associations, inducing self-censorship and a chilling effect on dissent; and (ii) by using mandatory enrolment requirements to exclude CSOs, their staff and their communities from the digital platforms essential for modern organising. As Sesan and Roberts highlight, digital ID systems in Africa carry inherent risks in that they can be used to "profile, discriminate against, target, and control citizens," while "high-risk applications such as surveillance or political profiling are advancing without adequate safeguards."[30] The consequence is that when mandatory enrolment is not accompanied by genuine opt-out options or alternative ways to verify identity, civil society actors can find themselves locked out of the digital ecosystems that enable advocacy and collective action, and deprived of the tools to communicate, organise, or demand accountability.

For the reasons outlined above, DPI must be understood as a form of constitutional and civic infrastructure. In the same manner as traditional public institutions such as courts, legislatures, and electoral bodies define the institutional architecture of democracy, DPI also defines the digital architecture through which rights are exercised and public authority is mediated. The design and governance of these systems therefore require strong legal safeguards, transparent oversight, and meaningful participation from civil society.

29 G Sesan & T Roberts 'Digital-ID in Africa: Assessing Progress and Challenges to Date', in 'G. Sesan and T. Roberts (eds), Biometric Digital-ID in Africa: Progress and Challenges to Date - Ten Country Case Studies 14-42.

30 As above 29-30.

3.2 Towards Civil Society Engagement

Just as traditional constitutional systems define the structures and limits of political power, DPI establishes digital rules and infrastructures that govern the exercise of authority and citizen engagement with state institutions in the digital age.[31] Data Privacy Brasil asserts that :for those of us in the Global South, DPI is not a neutral technical fix. It is the very infrastructure that defines how people access healthcare, education, and even basic citizenship rights."[32] Therefore, decisions about the design, governance, and oversight of DPI have profound implications for civic engagement, inclusion, democratic accountability, privacy, and the protection of fundamental rights. Given these implications, civil society is a relevant actor, considering its unique positioning to monitor, advocate for, and hold accountable the systems that produce these implications.[33] Essentially, in any constitutional order, principles require guardians. Those most vulnerable to governance failures such as the marginalised and historically excluded communities, rarely have direct access to where DPI is designed, which uniquely positions civil society as the relevant intermediary.

Understanding DPI as governance infrastructure is essential. In the absence of adequate safeguards, transparency, and oversight, DPI systems can reinforce inequalities, enable undue surveillance, or centralise power in ways that undermine democratic governance.[34] Conversely, when designed with strong human rights protections and participatory governance mechanisms, DPI can strengthen state capacity, expand civic participation, and enhance accountability.[35] This is why civil society has an essential role to play in shaping DPI governance. The role of civil society in the broad DPI ecosystem is explicitly acknowledged by the United Nations Development Programme (UNDP), which calls for investing in CSOs, Non-Governmental Organization (NGOs) and academic institutions to build knowledge, create informed and transparent debate and hold governments accountable for how DPI is planned, deployed and implemented."[36]

31 *See G Tusseau (2023). Taking Chaos Seriously: From Analog to Digital Constitutionalism (Chair of Digital, Governance and Sovereignty Working Paper). Sciences Po Law School 4 https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/11/chaire-digitale-g-tusseau-consitutionalism.pdf (accessed 5 May 2026).*

32 *Data Privacy Brasil:'The Global DPI Summit: reframing the debate from a Global South perspective' https://www.dataprivacybr.org/en/documentos/the-global-dpi-summit-reframing-the-debate-from-a-global-south-perspective-2/?idProject=1719 (accessed 5 May 2026).*

33 *R Onyango Digital Impact Alliance. (9 October 2025). The People's Network: Civil Society Organizations in Digital Public Infrastructure Development in Africa https://dial.global/research/civil-society-dpi-africa/#content (accessed 5 May 2026).*

34 *S de Carvalho Homem 'From Innovation to Inclusion? The Human Rights Dilemma of Digital Citizenship' (2026) https://www.shs-conferences.org/articles/shsconf/abs/2026/03/shsconf_ichss2026_01001/shsconf_ichss2026_01001.html (accessed 5 May 2026).*

35 *R Chandrasekhar et al 'Principles and Practices for Governing Digital Public Infrastructure (DPI) as Commons' (2025) Paper presented at the OpenForum Academy Symposium 2025, Rio De Janeiro, Brazil. https://doi.org/10.5281/zenodo.17539167 (accessed 6 May 2026).)*

36 *UNDP: 'Seizing the digital moment: From interlocking challenges to interoperable solutions' 2 September 2022 seizing-digital-moment-interlocking-challenges-interoperable-solutions (accessed 6 May 2026).*

4. Why Civil Society Must Engage

Civil society engagement in the development and governance of DPI is essential because these systems increasingly determine how citizens access services, interact with the state, and exercise their rights. When CSOs engage proactively, before and during the design and deployment of DPI, they can help prevent exclusion, mitigate risks of surveillance and data misuse, and ensure that systems are designed to serve the public interest instead of concentrating power in state or corporate actors. Although DPI systems such as digital identity platforms, interoperable data exchanges, and digital payment infrastructures can significantly expand access to public services and economic opportunities, without strong safeguards they may also create new forms of discrimination, exclusion, and rights violations. When digital systems centralise vast amounts of citizen data without effective oversight, they may enable mass surveillance or political manipulation. For these reasons, CSO engagement throughout the lifecycle of DPI is essential. Through advocating for transparency, privacy protections, inclusive design, and meaningful public participation, civil society can help ensure that DPI systems empower citizens, protect fundamental rights, and strengthen democratic governance rather than reinforcing exclusion or enabling unchecked surveillance.

5. Building CSO Capacity for Effective Engagement

It is on this established basis that civil society cannot wait until DPI systems are deployed to react. In order to protect rights, expand civic space, and influence the development of the digital state, CSOs must act upstream across multiple stages of the policy and technology lifecycle.[37] However, before any meaningful engagement can occur, CSOs must have the capacity to understand, shape and navigate DPI systems.

The civil society landscape is highly diverse, encompassing large advocacy organisations with dedicated digital rights units, grassroots community groups operating with limited resources, faith-based networks, women's associations, environmental justice collectives, and many others. In this broad spectrum, capacity is not automatically present. It must be deliberately built through digital literacy programmes that demystify the entire DPI discourse, including its technical architectures, governance models, data flows, legal frameworks, impact and intersectionalities such as those related to vulnerability, inclusion and marginalisation. Targeted capacity-building initiatives, peer learning networks, and technical partnerships with researchers and digital rights practitioners can further equip CSOs to navigate the complexities of DPI.[38]

For instance, in Kaduna State, Nigeria, CSOs and media practitioners received targeted capacity-building to use a newly launched AI-powered open contracting portal hosting over 1,000 infrastructure projects, with the government committing to strengthen social accountability through disclosed data.[39] This intervention occurred as the portal was being rolled out, enabling CSOs to engage with the DPI system from its early stages rather than reacting to failures after deployment. With such capacity in place, CSOs are better positioned to promote transparency, demand accountability, and safeguard human rights across every stage of DPI, from design to deployment, implementation to monitoring, and redress to reform.

37 Datasphere: 'Moving fast together: How sandboxes can help build trust in Digital Public Infrastructure' https://www.thedatasphere.org/news/moving-fast-together-how-sandboxes-can-help-build-trust-in-digital-public-infrastructure/#content (accessed 6 May 2026).)

38 For instance, the Thrive Digitalisation Project, implemented by HorizonT3000 in East Africa (Uganda, Kenya, and Tanzania), has been instrumental in strengthening digital capacities of local CSOs through training in digital monitoring and evaluation, online facilitation, data privacy and protection, among others. See https://www.horizont3000.org/en/articles/thrive-digitalisation-project (accessed 10 May 2026).

39 'Kaduna govt commits to strengthening social accountability in infrastructure sector' 23 June 2025 Peoples Gazette Nigeria https://gazettengr.com/kaduna-govt-commits-to-strengthening-social-accountability-in-infrastructure-sector/ (accessed 10 May 2026).

6. CSO Roles in the DPI Lifecycle

CSOs can exercise their participatory and oversight roles across the DPI lifecycle, grounded in the digital and governance expertise that enables effective action.

6.1 At the Design Stage

CSOs can participate in national planning processes for digital identity, digital payment platforms, and interoperable government systems through advocating for inclusion, equity, and human rights considerations from the outset. This means engaging with ministries, technical working groups, and donor consultations before technical specifications are locked in.[40] CSOs can demand Human Rights Impact Assessments (HRIAs) prior to deployment of systems as a means to identify risks related to privacy, exclusion, and civic participation, and use the findings to push for safeguards and mitigation measures drawing on comparative good practices from across the continent and globally.[41]

During the East Africa Internet Governance Forum (EA-IGF) held in Nairobi in May 2025, CSO participants reported that civil society has achieved significant victories across Africa by focusing on issues such as data governance, data protection, and privacy. However, the same revealed significantly lower CSO engagement on digital identity and payments, components that are "at the core of how DPI is operationalized." As the report notes, this mirrors patterns seen in Kenya's Huduma Namba and Uganda's Ndaga Muntu, "where civil society raised critical concerns about exclusion, surveillance, and consent, but only after the rollouts had begun and communities were already being harmed."[42]

This underscores why upstream engagement at the design stage is essential. CSOs can also advocate for availability of parallel analogue options during digital transitions, ensuring that individuals without digital literacy, reliable connectivity, or proper documentation are not excluded from essential services. This includes pushing for mobile enrolment agents and alternative verification methods for vulnerable populations such as the elderly, persons with disabilities, and remote communities. In Kenya, CSOs successfully advocated for constitutional and legal safeguards before the full implementation of the Huduma Namba digital ID system, resulting in stronger data protection measures and clearer legal frameworks through strategic litigation and advocacy.[43]

40 United Nations Development Programme: Accelerating The SDGgs Through Digital Public Infrastructure https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-g20-accelerating-the-sdgs-through-digital-public-infrastructure.pdf (accessed 10 May 2026).

41 UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights and related guidance on Human Rights Impact Assessments, 2011.

42 Digital Impact Alliance: R Onyango 'Are we really advancing together?" At the East Africa Internet Governance Forum, we sought to answer this critical question' 9 June 2025 https://dial.global/civil-society-dpi-at-east-africa-igf/#content (accessed 10 May 2026).

43 This is explicitly highlighted in the Nubian Rights Forum & 4 others v. Attorney General & 6 others (2020) case.

6.2 During Procurement and Deployment

Procurement oversight is a key but often neglected lever. CSOs can ensure that technology vendors meet transparency, security, and privacy-by-design standards while promoting open tendering and independent audits.[44] This requires CSOs to develop technical capacity to analyse contracts, assess vendor track records, and identify potential conflicts of interest. In contexts where procurement lacks transparency, CSOs can use access to information laws to request procurement documents and hold public officials accountable.

In Uganda, the Public Procurement and Disposal of Public Assets Authority (PPDA) formally onboarded CSOs, including the Anti-Corruption Coalition Uganda and the Uganda Debt Network, onto its digital Contract Monitoring System, enabling real-time tracking of government contracts to eliminate substandard works, prevent ghost payments, and reduce abandoned projects.[45] In Sierra Leone, the National Public Procurement Authority has partnered with the Budget Advocacy Network to launch a technology-driven initiative for civil society-led procurement monitoring, with digital tools making procurement processes more open, accessible, and citizen-focused.[46] These examples demonstrate that when CSOs are equipped with digital oversight tools and are formally integrated into procurement governance, they become effective watchdogs for transparency and accountability across the entire DPI lifecycle.

6.3 At the Policy and Legislative Level

CSOs can exercise legislative influence, advocating for strong rights protections in laws and regulations governing DPI, including clear limits on data use and sharing, meaningful consent requirements, and independent oversight mechanisms. This includes engaging with parliamentary committees, submitting legislative proposals, and mobilising public support for rights-protective frameworks.

Several examples demonstrate how CSOs are beginning to fulfill this role in Africa. In Kenya, Amnesty International launched Data Protection Guidelines for CSOs, positioning civil society as "stewards of digital rights and public trust" while also revealing that most citizens, particularly rural and marginalised communities are unaware of their data rights, underscoring the preparedness gap.[47] In Nigeria, civil society participated in multi-stakeholder workshops to shape the draft Online Harm Protection Bill, which proposes establishing a Multi-Stakeholder Council for participatory decision-making and an Independent Oversight Forum for transparency.[48] In Sierra Leone, nationwide consultations on the draft Data Protection Bill explicitly included civil society alongside government and private sector representatives, with officials noting that such inclusive approaches reflect principles of participatory governance.[49] In Senegal, sustained civil society advocacy

44 *World Bank, GovTech Procurement Practice Note: Technology Procurement for Digital Government, 2020. https://documents1.worldbank.org/curated/en/789261619416085415/pdf/GovTech-Procurement-Practice-Note-Summary-Note.pdf (accessed 10 May 2026).*

45 *Public Procurement and Disposal of Public Assets Authority: 'PPDA Onboards ACCU and UDN onto the Contract Monitoring System' 5 August 2025 https://www.ppda.go.ug/ppda-onboards-accu-and-udn-onto-the-contract-monitoring-system/ (accessed 10 May 2026).*

46 *S Jallow 'NPPA and Budget Advocacy Network Launch Tech-Driven Initiative' 30 January 2026 https://a-zsl.com/nppa-and-budget-advocacy-network-launch-tech-driven-initiative/#respond (accessed 10 May 2026).*

47 *Amnesty International: 'Amnesty International Kenya Launches Landmark Study and Guidelines on Data Protection to Strengthen Digital Rights And Accountability In Kenya' 2 October 2025 amnesty-international-kenya-launches-landmark-study-and-guidelines-on-data-protection-to-strengthen-digital-rights-and-accountability-in-kenya (accessed 10 May 2026).*

48 *National Information Technology Development Agency:J Ishaku 'Nigeria Advances Citizen Led Digital Governance With Online Harm Protection Bill' 25 July 2025 https://nitda.gov.ng/nigeria-advances-citizen-led-digital-governance-with-online-harm-protection-bill/9037/ (accessed 10 May 2026).*

49 *'Ministry Launches Consultations on Data Protection Law' 13 September 2025 Africa Press https://www.africa-press.net/sierra-leone/all-news/ministry-launches-consultations-on-data-protection-law#respond (accessed 10 May 2026).*

over nearly two decades culminated in the adoption of the Access to Information Law in August 2025. ARTICLE 19 led much of this advocacy which culminated in a progressive access to information law when compared to other countries in Francophone West Africa.[50] This role has since extended to the post-adoption phase to monitor implementation.

Beyond formal legislation, CSOs can engage continental human rights bodies to advance DPI accountability. In this regard, civil society can advocate for institutionalised multistakeholder governance mechanisms that give civil society a sustainable, permanent role, rather than tokenistic adhoc consultations. The African Commission on Human and Peoples' Rights (ACHPR) has a significant role to play in this regard, providing guidance, oversight, and accountability in the design and deployment of DPI across the continent. CSOs are uniquely positioned to act as intermediaries between citizens and the state, leveraging ACHPR frameworks to advocate for digital governance that aligns with human rights standards.[51]

However, as presented at the 2025 Global DPI Summit,[52] media coverage on DPI generally in African countries is substantially reliant on official government sources and there is limited attention to civil society dimensions on DPI.[53] This suggests that while CSOs are present in legislative processes, their capacity to shape public discourse and mobilise support for rights-protective frameworks is still underdeveloped. This is a gap that targeted capacity-building and strategic communications support could address.

6.4 Throughout Implementation and Operations

Ongoing monitoring and accountability efforts are essential. CSOs can track DPI rollout and its impact on rights, submit shadow reports to parliament and international human rights bodies including the ACHPR, request thematic hearings, or pursue strategic litigation where necessary. This requires establishing baseline data before deployment against which to measure changes in access, exclusion rates, and rights violations.

In South Africa, efforts to digitise social protection delivery have been met with concerns about language barriers, low digital literacy, and trust. CSOs have played a key role in documenting these challenges and advocating for more inclusive design. Research from the Institute of Development Studies found that digital systems frequently exclude vulnerable populations through design choices prioritising efficiency over rights, a phenomenon termed 'accountability displacement'.[54] Similarly, civil society groups like Black Sash and #PayTheGrants have documented how mandatory online biometric verification disproportionately affects those

50 *Rule of Law Lab:'Rule of Law Lab and Article 19 Senegal and West Africa Welcome Access to Information Bill, Urge Alignment with International Standards' 19 August 2025 https://www.law.nyu.edu/rule-law-lab/press-release-senegal-access-information-law (accessed 10 May 2026).*

51 *H Dube 'Safeguarding Human Rights in Africa's Digital Transformation: The Role of the ACHPR in DPI Governance' 23 March 2026 AfricLaw https://africlaw.com/2026/03/23/safeguarding-human-rights-in-africas-digital-transformation-the-role-of-the-achpr-in-dpi-governance/. The ACHPR has adopted relevant resolutions for monitoring human rights in the digital age, including resolutions on elections, access to data, among others, that are relevant for DPI advocacy.*

52 *For 2025 DPI Global Summit, see: https://www.globaldpisummit.org/ (accessed 10 May 2026).*

53 *Paradigm Initiative: 'Centering human rights in the design and adoption of DPIs: Perspectives on DPI design, adoption and implementation' 14 January 2026 https://paradigmhq.org/centering-human-rights-in-the-design-and-adoption-of-dpis-perspectives-on-dpi-design-adoption-and-implementation/ (accessed 10 May 2026).*

54 *Institute of Development Studies: C Khene et al.'Beyond Digital Displacement: Accountability in South Africa's Digitalised Social Protection System (2025) https://opendocs.ids.ac.uk/articles/report/Beyond_Digital_Displacement_Accountability_in_South_Africa_s_Digitalised_South_Protection_System/30819806?file=60182849 (accessed 10 May 2026).*

without smartphones or internet access, and have called for transparency regarding the opaque algorithmic decision-making that can suspend a person's only source of income.[55]

Although some African CSOs are already performing commendable monitoring and accountability functions, there are few that focus specifically on independent evaluation of DPI systems. There is therefore a need for sustained investment in CSO preparedness, including baseline data collection and systematic rights monitoring from the earliest stages of DPI deployment.

6.5 Through Strategic Litigation and Legal Accountability

Where other avenues fail, CSOs can turn to the courts. Strategic litigation can challenge unconstitutional aspects of DPI systems, compel governments to enforce data protection and access to information laws, or establish legal precedents that protect citizens' rights. This requires CSOs to build partnerships with public interest law firms, legal aid organisations, and human rights lawyers across the continent. African CSOs have used strategic litigation to hold DPI systems accountable.

In Kenya, CSOs raised concerns about the potential risks associated with the government's digital identity initiative. Advocacy and litigation highlighted issues related to data protection, exclusion of marginalised groups lacking documentation, and the absence of effective legal safeguards.[56] The Nubian Rights Forum, Kenya Human Rights Commission, and Katiba Institute challenged the Huduma Namba digital ID rollout. In a January 2020 judgment, the mandatory collection of DNA and GPS coordinates was declared unconstitutional as a disproportionate violation of the right to privacy under Article 31 of the Kenyan Constitution.[57] The court allowed the Huduma Namba system to proceed only after the government had operationalised a comprehensive regulatory framework under the newly enacted Data Protection Act, 2019, to safeguard against data misuse. Consequently, courts required the government to strengthen data protection measures and establish clearer legal frameworks before fully implementing the system.[58] This case illustrates how CSOs can use strategic litigation to hold DPI initiatives accountable to constitutional rights and international human rights standards, turning court rulings into tangible protections for citizens.

55 *Black Sash: 'Universal Basic Income Coalition is concerned about the apparent deepening of digital hurdles to accessing the SRD Grant' 24 June 2024 https://www.blacksash.org.za/universal-basic-income-coalition-is-concerned-about-the-apparent-deepening-of-digital-hurdles-to-accessing-the-srd-grant/ (accessed 10 May 2026).*

56 *See https://digitalfrontiersinstitute.org/recording/listen-now-kenyas-huduma-namba-risks-responses-and-the-fight-for-genuine-inclusion/ (accessed 10 May 2026).*

57 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR (Constitutional Petitions No. 56, 58 & 59 of 2019, consolidated).*

58 *As above.*

In Nigeria, the Laws and Rights Awareness Initiative sued the National Identity Management Commission, alleging that its digital ID mobile app was insecure and breached Nigerians' constitutional right to privacy, citing evidence of data breaches within 48 hours of the app's release.[59] In Uganda, the Unwanted Witness submitted a formal petition to the Uganda Human Rights Commission documenting financial barriers, exclusion of vulnerable groups, and NIRA's expired data protection registration.[60] In South Africa, Black Sash has publicly challenged SASSA's grant review process, arguing that beneficiaries were cut off without due process, while prior court rulings found that algorithmic profiling and database cross-checking were 'intentionally exclusionary' and that 9 out of 10 people excluded were wrongfully denied.[61] These examples demonstrate that strategic litigation is an important tool for CSOs to enforce implementation and challenge the constitutionality of laws, which compels DPI accountability, and establishes legal precedents that protect citizens' rights.

6.6 Through Capacity Building and Public Education

Public education and awareness campaigns empower communities to understand their digital rights, participate safely in DPI systems, and hold authorities accountable in the various phases of the DPI lifecycle. Through trusted community intermediaries, including faith-based organisations, women's self-help groups, farmer cooperatives, and youth networks, CSOs can build digital literacy, demystify how DPI systems function, explain available legal protections, and create accessible feedback channels, which could potentially strengthen community preparedness for DPI deployment.

Research across African contexts reveals potential entry points for such CSO-led efforts.[62] For instance, marginalised populations often struggle to register for biometric digital IDs due to challenges such as disability, illiteracy, or costs such as mobile data and phone access. CSOs have the potential to address these gaps by strengthening understanding of the DPI lifecycle, raising awareness of data protection frameworks, advocating for accessible complaint mechanisms, and educating communities on redress procedures when DPI systems fail, whether through data breaches, system errors, or wrongful exclusion from services.[63] This role enables CSOs to exercise preparedness, watchdog, and advocacy functions throughout the DPI lifecycle, helping ensure that DPI systems are accountable to citizens from design through sunsetting.

59 'Digital ID Card: CSO Drags NIMC To Court' Oasis Magazine 19 August 2020 https://oasismagazine.com.ng/2020/08/digital-id-card-cso-drags-nimc-to-court/ (accessed 10 May 2026).

60 Unwanted Witness: 'Unwanted Witness Submits Petition to Uganda Human Rights Commission Regarding National ID System' 30 July 2024 https://www.unwantedwitness.org/unwanted-witness-submits-petition-to-uganda-human-rights-commission-regarding-national-id-system/ (accessed 10 May 2026).

61 Black Sash: 'Universal Basic Income Coalition is Concerned about the Apparent Deepening of Digital Hurdles to Accessing the SRD Grant' 24 June 2024 https://www.blacksash.org.za/universal-basic-income-coalition-is-concerned-about-the-apparent-deepening-of-digital-hurdles-to-accessing-the-srd-grant/ (accessed 10 May 2026).

62 Citizenship Rights in Africa Initiative documented biometric digital ID implementation challenge and researchers noted the challenges which creates strategic entry points for CSOs in providing the requisite capacity and awareness. See https://citizenshiprightsafrica.org/en/biometric-digital-id-in-africa-progress-and-challenges-to-date-ten-country-case-studies/ (accessed 12 May 2026).

63 As above.

Summary Table: CSO Roles Across the Lifecycle

Design

Participate in planning; demand HRIAs; advocate for analogue alternatives and redress mechanisms

Procurement

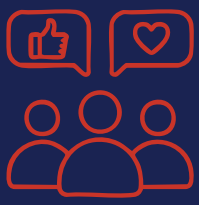
Oversee vendor contracts; demand transparency and privacy-by-design; use Integrity Pacts to prevent bribery, fraud and collusion in public procurement

Policy

Influence legislation; push for multistakeholder governance; advocate for CSO seats on oversight bodies

Implementation

Monitor rollout; document exclusions; submit shadow reports; undertake strategic litigation



Participation

Facilitate community consultations; create feedback loops; ensure sustained engagement

Capacity building

Train CSO staff; build digital literacy; roll out public education campaigns

7. Institutional Landscape for CSO Preparedness

Beyond internal capabilities, CSO preparedness also requires strategic mapping of the institutional actors that shape DPI governance. By understanding which actors hold leverage at each stage of the DPI lifecycle, CSOs can target their advocacy, build relationships, and act decisively when opportunities or threats arise. The following categories of institutional actors are particularly pertinent entry points for CSO engagement:

Policy and implementation agencies

Policy submissions, advisory processes

Data protection authorities

Complaints, investigations, consultations

Legislative bodies

Testimony, legal briefs, amendment advocacy

Procurement & treasury

Monitoring, disclosure advocacy

National Human Rights Institutions

Shadow reports, complaints, consultations

Private sector

Contract safeguards, open standards advocacy

Sector regulators

Complaints, shadow reports, policy reviews

7.1 Policy and Implementation Agencies

Ministries responsible for Information and Communication Technology (ICT), digital economy, or innovation lead national digital transformation strategies and oversee core DPI systems such as digital identity platforms and e-government services from government ministries, departments and agencies like those responsible for justice, business registration and finance. CSOs can engage these ministries through policy consultations, submissions, and multi-stakeholder advisory processes. Digital transformation or e-government agencies manage the technical architecture and operational implementation of DPI. CSOs can advocate for privacy-by-design, inclusive system architecture, and transparency measures during design and deployment stages.[64]

7.2 Data Protection Authorities (DPAs)

DPAs regulate the collection, processing, and sharing of personal data in DPI ecosystems. CSOs can submit complaints, request investigations, contribute to regulatory consultations, and collaborate on public awareness initiatives about digital rights and data governance.[65]

7.3 Legislative Bodies

Parliamentary committees responsible for ICT, governance, or human rights shape the legal frameworks governing DPI. CSOs can provide expert testimony, submit policy briefs, and advocate for amendments that strengthen safeguards and accountability provisions in DPI-related laws.[66]

7.4 Public Procurement and Treasury Departments

DPI systems are often implemented through large-scale technology contracts with private vendors. CSOs can promote transparency by monitoring procurement processes, advocating for open tendering and contract disclosure, and raising concerns about vendor practices that undermine privacy or public interest safeguards.[67]

64 Examples of CSO engagement with policy and implementation agencies in Africa include: ID4Africa, a Pan-African movement with 48 member states, has institutionalised civil society participation in digital identity governance, including dedicated plenary sessions on CSO contributions to inclusive and rights-respecting identity systems. More information here: https://id4africa.com/ In South Africa, the Department of Communications and Digital Technologies (DCDT) maintains multi-stakeholder consultation processes for ICT policy development, with civil society participating alongside industry, academia, and thought leaders. See S Mzekandaba 'SA ICT policy must hasten move to 'execution' stage' 29 November 2024 https://www.itweb.co.za/event/GRC2025/content/PmxVEMKEj6nvQY85/index.html

The Africa Internet Governance Forum (AfIGF)provides a structured multi-stakeholder platform where CSOs engage with policy and implementation agencies on digital governance, data protection, and connectivity issues, supported by national IGFs in Africa. For more information see here: https://registry.africa/fr/africa-internet-governance-forum-afigf/ (accessed 12 May 2026).

65 For instance: Nigeria Data Protection Commission: ''NDPC, CSOs to Partner on Advancing Data Privacy and Digital Rights Across Nigeria' 6 November 2025 https://ndpc.gov.ng/ndpc-csos-to-partner-on-advancing-data-privacy-and-digital-rights-across-nigeria/#respond (accessed 10 May 2026).

66 There are many examples on the continent such as: In Nigeria, Paradigm Initiative and Avocats Sans Frontières organised a legislative retreat with the National Assembly on the Digital Rights and Freedom Bill, bringing together parliamentarians and CSOs to strengthen rights-based digital legislation. More information available here: B Nwannekanma 'Stakeholders harp on minors' protection at digital rights bill discourse' (25 November 2025) The Guardian Nigeria https://guardian.ng/features/law/stakeholders-harp-on-minors-protection-at-digital-rights-bill-discourse/.

In Uganda, Unwanted Witness engaged parliamentary committees throughout the legislative process leading to the Data Protection and Privacy Act, 2019, providing expert testimony and building technical capacity among lawmakers. For more information: D Mukasa D 'Lived experience of advocating for data protection in Uganda' African Declaration on Internet Rights and Freedoms (2024) https://africaninternetrights.org/ar/node/2534 3) (accessed 12 May 2026).

67 See, for example, the Africa Freedom of Information Centre's multi-country project (Kenya, Malawi, Uganda, Nigeria) which trained CSOs on open contracting, created contract monitoring dashboards, and led the Government of Uganda to launch a formal CSO contract monitoring framework in 2019. Available here: Africa Freedom of Information Centre: 'Picking lessons from strengthening disclosure and citizen participation in public contracting in Africa: A case of Uganda, Kenya, and Nigeria' 7 September 2020 https://www.africafoicentre.org/picking-lessons-from-strengthening-disclosure-and-citizen-participation-to-improve-value-for-money-in-public-contracting-in-africa-a-case-of-uganda-kenya-and-nigeria/ (accessed 12 May 2026).

7.5 National Human Rights Institutions (NHRIs)

NHRIs are central players in integrating human rights safeguards into DPI systems. Their mandate positions them as natural oversight bodies for digital systems affecting privacy, non-discrimination, and service access.[68] NHRIs can mandate HRIAs before DPI deployment, provide complaint mechanisms for affected citizens, and independently monitor implementation against constitutional and international standards. CSOs can engage NHRIs by submitting shadow reports, filing complaints, and participating in NHRI-led consultations. While the ACHPR is currently not actively engaged in DPI governance, its human rights framework offers principles that CSOs and NHRIs can apply for guidance and accountability.[69]

7.6 The Private Sector

The private sector is an essential but complex partner in DPI rollout. CSOs must be vigilant against several risks:

Summary[70]

Market concentration
A single entity dominates DPI infrastructure, creating data hegemony

Data extractivism
Private entities monetise citizen data beyond service delivery needs

Vendor lock-in
Government dependence on proprietary technology undermines digital sovereignty

Exclusion
Profitable urban or formal-sector users are prioritised over marginalised communities

Regulatory blind spots
Private partners operate in gaps between sector regulators

CSO preparedness requires advocating for contractual safeguards, open standards, interoperability, and multi-stakeholder oversight that includes civil society representation.

68 *Office of the United Nations High Commissioner for Human Rights: 'Public policy and digital technologies: The role of National Human Rights Institutions in achieving policy coherence' (2021) B-Tech Blog https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-blog-policy-coherence-nhris-tech.pdf (accessed 12 May 2026).*

69 *n 51 above.*

70 *Some of the aspects in this table are synthesised from expert analysis from the IGF 2025 Workshop WS #257: Data for Impact: Equitable & Sustainable DPI Data Governance, Session Report (24 June 2025), discussing risks including data extractivism, monopolistic control of DPI through network effects, and "regulatory blind spots" where private entities operate on public platforms without adequate oversight. See the official session transcript and recording here: https://info.intgovforum.org/en/content/igf-2025-day-1-workshop-room-2-ws-257-data-for-impact-equitable-sustainable-dpi-data (accessed 12 May 2026).*

7.7 Sector Regulators

Telecommunications and financial services authorities influence how DPI affects digital access, financial inclusion, and rights. CSOs can submit complaints, produce shadow reports, and advocate for investigations or policy reviews where DPI raises concerns about privacy, discrimination, or surveillance. In Tanzania, the Digital Agenda for Tanzania Initiative (DA4TI), produced a report identifying data protection loopholes in the country's biometric SIM card registration drive. The report called on mobile network operators to adhere to privacy commitments, criticised the government's failure to establish a data protection authority as required by the Personal Data Protection Act, and urged all stakeholders to uphold data privacy standards.[71] This is an example of a CSO submitting evidence to successfully influence telecommunications regulators and data protection authorities on privacy concerns in a biometric registration system linked to mobile services.

By understanding the institutional landscape and engaging strategically with these actors, CSOs can move beyond reactive advocacy and influence DPI at every stage. This proactive engagement enables them to contribute to governance frameworks, strengthen accountability mechanisms, and ensure that DPI systems are transparent, inclusive, and aligned with democratic values and human rights principles.

71 *Digital Agenda for Tanzania Initiative: 'Biometric Identity, SIM Card Registration, and Telecoms in Tanzania' (2023) https://greaterinternetfreedom.org/publication/country-report-biometric-identity-sim-card-registration-and-telecoms-in-tanzania/ (accessed 10 May 2026).*

8. Key Question for CSOs

A central question should guide civil society engagement with DPI:
Is DPI being designed to empower citizens and strengthen democratic participation, or is it consolidating state or private control over people's identities, data, and civic life?

This question reflects the fundamental tension at the heart of digital governance. While DPI systems have the potential to expand access to services, improve transparency, and strengthen civic participation, they can also create powerful mechanisms for centralized control over identity, information, and public participation if not designed and governed with strong safeguards. For CSOs, this question should serve as a practical framework for evaluating DPI initiatives at every stage of their lifecycle, including policy development, system design, implementation, and oversight. Each new digital identity system or infrastructure should be examined through a set of pertinent questions:

a. Who controls the data generated by these systems?
b. What safeguards exist to protect privacy and prevent misuse?
c. Are the systems inclusive and accessible to marginalised populations?
d. Do citizens have meaningful mechanisms to challenge errors, misuse, or exclusion?
e. Are there independent institutions capable of providing oversight and accountability?

Framing engagement around these core questions enables CSOs to move beyond reactive responses to technological change and adopt a principled, rights-based approach to digital governance. Consistently interrogating whether DPI systems expand public participation or concentrate control, civil society can identify potential risks early, advocate for necessary safeguards, and promote governance models that prioritise transparency, accountability, and inclusion.

The response to these questions determines whether DPI becomes a tool for democratic empowerment or whether it undermines it. For civil society, maintaining vigilance around this balance is essential to ensuring that the digital transformation of governance advances human rights and democratic values.

9. Call to Action

Having established that DPI is not neutral technology and that it is the architecture of citizenship in the digital age, decisions about how identity systems are built, how data is governed, and how digital platforms mediate public life, shapes visibility to the state, access to services, and meaningful public participation.

For civil society across Africa, the stakes are profound considering that DPI systems are being designed and deployed at unprecedented speed, often with limited public scrutiny. If these systems are developed without effective safeguards, they risk concentrating power, enabling undue surveillance, and excluding vulnerable and marginalised communities. However, if governed transparently and grounded in human rights principles, DPI can strengthen democratic participation, improve service delivery, and expand civic inclusion. Therefore, civil society cannot afford to engage only after these systems are already integrated in governance. The ideal moment for engagement is upstream, during policy design, legislative debates, procurement processes, and system architecture decisions. Across the continent, CSOs must therefore act not as passive observers of digital transformation, but as active shapers of the digital state.

10. Immediate Action Steps for Civil Society

To effectively influence the development of DPI, CSOs should adopt a coordinated, rights-based strategy, which entail the following:

Build Technical and Legal Capacity:
Develop expertise in digital governance, data protection, cybersecurity, and DPI architecture. Strengthening internal capacity enables CSOs to engage meaningfully in technical and policy discussions.

Research and Engage Early in Policy and System Design:
Recognising that governments may not always be open or inclusive of CSOs from the outset, CSOs must first proactively research and stay abreast of developments in DPI and of engagement opportunities, including draft bills, public notice periods, donor-led forums, and parliamentary inquiries. Where opportunities are identified, CSOs should participate in consultations, legislative processes, and technical working groups related to digital identity, data governance, and digital public services. Early engagement is critical to integrating inclusion, transparency, and rights protections.

Monitoring Implementation and Accountability
Civil society must equip its representatives and stakeholders to track DPI rollouts, procurement processes, and data governance practices. This includes using tools such as shadow reporting, parliamentary engagement, and strategic litigation to hold authorities accountable where necessary.

Examples of initiatives that CSOs may undertake include:

i. Educate and Empower Communities
ii. Promote digital rights literacy so that citizens understand how DPI systems affect their rights, participation, and access to services. Public awareness strengthens democratic oversight
iii. Strengthen Regional Collaboration
iv. Build coalitions across the continent to share expertise, coordinate advocacy, and leverage regional human rights frameworks such as the African Charter on Human and Peoples' Rights, the Malabo Convention, and other relevant international, continental and regional standards
v. Partner with media organisations, including investigative journalism networks, community radio stations, and digital rights media platforms, to promote public awareness of DPI systems, expose data breaches or exclusionary practices, and amplify citizen voices in digital governance debates. Media partnerships strengthen democratic oversight by translating technical DPI issues into accessible public knowledge.

11. Conclusion

Civil society engagement in DPI is essential to the protection of fundamental rights. DPI systems determine how individuals are identified, access services, communicate with public institutions, and participate in democratic life, directly shaping how rights such as privacy, freedom of expression, association, and political participation are exercised or restricted. This reality creates an indispensable role for civil society. Drawing on international and regional human rights standards, CSOs act as interlocutors between citizens and the state, advocating for rights-respecting digital governance, demanding transparency, identifying risks of exclusion or undue surveillance, and holding institutions accountable. In this way, CSO engagement facilitates alignment of DPI development and governance with established human rights obligations rather than undermining them. Fulfilling this role requires preparedness. CSOs must build technical and legal capacity, map institutional landscapes, forge strategic partnerships, and engage upstream in policy and design processes. In the formative period of Africa's digital state, civil society must be among the authors of the digital compact.

This publication has been made possible with financial support from Norway through the International Center for Not-for-Profit Law (ICNL). The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the Government of Norway.