MAPPING GLOBAL DIGITAL PUBLIC INFRASTRUCTURE (DPI): A HUMAN RIGHTS PERSPECTIVE WITH FOCUS ON KENYA

International Commission of Jurists
KENYAN SECTION | Since 1959

Published by
The Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ICJ Kenya House, Off Silanga Road, Karen
P.O Box 59743 - 00200, Nairobi, Kenya
Tel: +254-20-2084836/8|+254 720 491549
Email: info@icj-kenya.org
Website: www.icj-kenya.org

Design and Layout:
Ndolo Anderson
Lead Graphics Designer & illustrator - ICJ Kenya

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to all those who contributed to the successful completion of this research work. This study would not have been possible without the dedication and hard work of our Research Consultant Henry Omusundi Maina who worked hand in hand with Jaika Charles Magotzwi, whose insightful research and analysis played a critical role in bringing this project to fruition.

Our deepest thanks go to Research Consultant Henry Omusundi Maina for conducting the research with meticulous attention to detail and commitment. Jaika, as the lead on this initiative, had the privilege of identifying the research topic and overseeing its development under the portfolio of Digital Rights, Civic Space, and Independent Media.

Additionally, we would like to acknowledge the invaluable contribution of our Deputy Executive Director, Demas Kiprono, whose efforts in editing and refining the research were crucial in ensuring its quality and clarity.

The collective input from everyone involved has made this research a success, and we are truly appreciative of the time, expertise, and support each of you provided.

Signed,

Erick Mukoya

Executive Director

ICJ Kenya.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Societies operate on infrastructures: physical, social, and digital. At the intersection of social and digital infrastructures is a set of spaces that host critical conversations about civic, political and social issues. At present, these spaces primarily built and governed by large private companies who maintain them to collect user data and serve advertisements among other uses. Physical, social and digital infrastructures generate externalities, both positive and negative.

Mapping Global Digital Public Infrastructure (DPI): A Human Rights Perspective with Focus on Kenya looks at the digital public infrastructure with a view to mitigate negative externalities. It offers a critical exploration of the intersection between digital transformation and human rights, with a particular emphasis on the Kenyan context. This report evaluates DPI as a cornerstone of modern governance, economic systems, and social interaction, while addressing its human rights implications internationally and locally.

DPI encompasses foundational technological systems that provide broad access to essential digital services, including digital identity platforms, financial systems, and secure data exchange frameworks. These infrastructures promise to accelerate socio-economic transformation, improve service delivery, and foster innovation.

However, their adoption also introduces significant challenges, particularly in contexts with limited governance and regulatory capacity. Globally, the tension between DPI's transformative potential and its risks—such as privacy violations, inequitable access, and governance gaps—is increasingly evident.

This report uses a human rights framework to analyze these dynamics, offering insights from both global experiences and Kenya's unique challenges. The report outlines key trends in DPI implementation worldwide, drawing on case studies from nations like Estonia, India, South Korea, Brazil, and the United States. These countries highlight the diverse approaches to leveraging DPI for societal benefits, as well as the associated risks. Regionally, the African context reveals both innovations and vulnerabilities.

Case studies from Nigeria, South Africa, Tanzania, Ethiopia, and Uganda illustrate how resource constraints and governance issues intersect with DPI deployment. Despite these challenges, there are promising initiatives demonstrating Africa's potential to harness DPI for inclusive growth.

Kenya is a critical focus of this report, representing both the promise and challenges of DPI in Africa. As a leader in digital innovation, Kenya has implemented initiatives like M-Pesa, eCitizen, and Huduma Namba, which showcase its potential to drive inclusion through DPI. However, these systems have also raised significant concerns regarding equity, accessibility, data privacy, and informed consent. The report dedicates particular attention to the Worldcoin project initiative in early 2022, which sparked controversy over biometric data collection and governance. This case study underscores the urgent need for robust regulatory frameworks to safeguard human rights while leveraging DPI for development. The deployment of DPI, while fostering connectivity and economic growth, can also exacerbate inequalities and violate fundamental rights if not implemented with a rights-respecting approach.

Key human rights concerns identified in this report include:

- **Privacy and Data Protection:** The lack of robust safeguards around personal data collection and storage, particularly concerning biometric data, poses significant risks to individual autonomy.
- **Equity and Accessibility:** Without intentional design, DPI initiatives risk excluding marginalized communities, deepening socio-economic divides.
- **Transparency and Accountability:** Gaps in governance and oversight can lead to misuse of DPI for surveillance or discrimination.

To address these challenges, the report provides actionable recommendations for policymakers and stakeholders.

Global Recommendations:

- Establish universal human rights-based principles for DPI design and implementation.
- Foster multilateral cooperation to create global data protection standards.
- Promote transparency in DPI projects, ensuring informed consent and public accountability.

Regional Recommendations (African Context):

- Strengthen regional collaboration to share best practices and develop localized DPI solutions.
- Invest in capacity building for regulatory bodies to address governance gaps.
- Prioritize inclusivity by designing DPI systems that accommodate the needs of marginalized groups.

Introduction

Digital Public Infrastructure (DPI) has become a cornerstone of modern governance, economic systems, and social interaction across the globe. Defined as foundational technological frameworks that enable broad access to essential digital services such as digital identification systems, financial payment platforms and systems, and secure data exchange mechanisms. DPIs can be a catalyst for economic growth as they foster innovation and international trade. DPIs play a crucial role in fostering international trade through improved cross-border transactions, interoperability of financial systems, and the facilitation of global e-commerce.[1] Furthermore, they spur innovation by providing a secure and scalable platform for businesses and entrepreneurs to develop new digital solutions, enabling greater collaboration and knowledge sharing across regions.

DPIs have the potential to drive significant socio-economic transformation. However, their implementation is frequently accompanied by complex human rights challenges, particularly in developing nations like Kenya, where governance structures and resource constraints pose unique barriers.

This report provides a comprehensive examination of DPI from a global perspective, using a human rights framework to assess its impact on accessibility, accuracy, equity, privacy, and ownership. It places particular emphasis on Kenya while incorporating international examples and localized contexts to explore the dual nature of DPIs: as catalysts for development and potential threats to fundamental rights.

The analysis highlights global DPI initiatives, incorporating case studies from countries including China, India, Estonia, Brazil, Ukraine, the United States, South Korea, and others, alongside African nations such as Tanzania, Nigeria, South Africa, Ghana, Ethiopia, Uganda, and Kenya as the focus country.

The report also places a critical emphasis on the Worldcoin project in Kenya, highlighting the risks tied to biometric data collection and concerns around what may constitute voluntary informed consent.

The report provides targeted recommendations for policy-makers to guide the development and implementation of DPIs, emphasizing the critical need to align such initiatives with human rights standards. It underscores the urgency of adopting inclusive, transparent, and rights-respecting approaches to ensure that DPIs deliver maximum benefits while mitigating potential risks for all stakeholders.

[1] Junwen Feng, Shoubin Qi. (2024). "Digital Infrastructure Expansion and Economic Growth in Asian Countries," Journal of Business and Economic Option (JBEO), Vol 7 No 2, ISSN: 3006-2888 (online), ISSN: 3006-287X (Print)

Global and Regional Overview of Digital Public Infrastructure

Without infrastructures, society does not operate well. These infrastructures may include water and sewerage systems, electricity grid, public road (highways, feeder network, rail network, transport companies among many others. Infrastructures are markers of development. Underdevelopment is defined in terms of absence of these infrastructures.

The UN's Sustainable Development Goals include three goals directly related to physical infrastructures (6. Clean Water and Sanitation, 7. Affordable and Clean Energy, 11. Industry, Innovation and Infrastructure) and at least two related social infrastructures (4. Quality Education, and 16. Peace, Justice and Strong Institutions.)[2] So from the above it is clear that infrastructures can be physical, and social.

So, what are digital infrastructure? Like other infrastructures, digital public infrastructure are the tools and systems required to make digital life function. They include the wiring and circuitry of the internet (maintained mostly by for profit telecom companies), institutions such as the domain name system (like ICANN and IANA), and the software that keeps the internet running (primarily open-source software). They also include tools we all need to use to make digital spaces accessible and usable. Search as DNS systems, internet peering arrangements, discovery systems such as Google and Bing can be understood as digital infrastructures, as can marketplaces for apps, such as Android and iTunes stores. Web browsers such as chrome (commercial) and Firefox (not profit) are infrastructural, as well.

Digital infrastructures can be social as well as economic or technical. Facebook has served as a near universal directory for people on the internet and has provided semi-public spaces to interact with those people.

Therefore, digital public infrastructures (DPI) are the infrastructure that let us engage in public and civic life in digital spaces.

1. Definition and Components of DPI

DPI typically comprises three foundational pillars:

Digital Identification Systems: Systems that authenticate and manage citizens' identities digitally, such as Aadhaar in India.

01

Digital Payment Systems: Platforms that facilitate cashless transactions, such as India's Unified Payments Interface (UPI) and Kenya's M-Pesa.

02

Data Exchange Platforms: Infrastructure that enables secure data sharing, such as Estonia's X-Road.

03

[2] United Nations Department of Economic and Social Affairs, "The 17 Goals." Available at https://sdgs.un.org/goals, Accessed on 10th Dec 2024.

2. Global Case Studies of DPI

- **India: Aadhaar, UPI, and DigiLocker**

India's DPI framework, built around Aadhaar, UPI, and Digi-Locker to serve as a model for many countries. Aadhaar Biometric ID System, which is the world's largest biometric ID system, provides a unique 12-digit identifier for over 1.3 billion residents. Decentralized identity systems can provide individual control over biometric data. While it facilitates access to government subsidies, enabled financial inclusion, and streamlined service delivery,[3] it has also raised concerns regarding privacy violations, exclusion (lack of accessibility), and potential surveillance. Critics point to cases of biometric authentication failures denying essential services to marginalized groups and the potential for state overreach in monitoring citizens.[4]

- **Estonia: e-Residency and X-Road System**

X-Road is a secure, interoperable data exchange system while the e-Residency is a global digital identity platform enabling access to Estonian e-services. It is believed that the blockchain-based systems can enhance transparency and ensure secure, verifiable data exchanges.[5] While praised for its transparency and data security protocols, critics warn of potential risks if such systems were replicated in less regulated or digitally less advanced contexts.[6] In these environments, the absence of robust digital infrastructure, limited cybersecurity measures, and insufficient regulatory frameworks could create significant vulnerabilities. For instance, poor digital literacy among users might lead to exploitation, while weak oversight mechanisms could increase the risk of fraud, data breaches, or misuse of the technology. Additionally, the high technical and financial demands of implementing blockchain systems could strain resources in such contexts, potentially widening digital inequalities.

- **China: Social Credit System**

Integrates data from financial, legal, and social sectors to assign scores to individuals and businesses. Though intended to promote trust and compliance, it has drawn substantial global criticism from global civil society organisations and UN agencies for its opaque algorithms, punitive nature, and potential to curtail fundamental freedoms, particularly for dissidents and marginalized groups.[7] Critics argue that such systems are incompatible with universal human rights principles, citing concerns over the disproportionate impact on dissidents and marginalized groups , the erosion of privacy rights, and the fostering of a surveillance-driven environment that undermines freedom of expression, assembly, and movement.

- **Ukraine: Diia Digital Government Platform**

Consolidates over 70 government services, including digital IDs, passports, COVID-19 vaccination certificates and welfare access. While it has been crucial during the war for displaced citizens as decentralized technologies can safeguard critical data during crises and ensure continuity of services,[8] concerns include cybersecurity vulnerabilities, privacy breaches, and equitable access for older citizens and rural populations.[9]

---

3 https://www.chandlerinstitute.org/governancematters/indias-aadhaar-system-bringing-e-government-to-life

4 Khera, R. (2019). "The Aadhaar Debate: A Critical Analysis of Privacy Concerns."

5 Margetts, H. (2020). "The Estonian Digital State: Lessons for the World."

6 https://policyreview.info/articles/analysis/estonias-digital-diplomacy-nordic-interoperability

7 https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist

8 OECD (2023). "Digital Resilience in Ukraine: Lessons for Future DPI."

9 https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-diia-platform-sets-the-global-gold-standard-for-e-government/

- **Brazil: Cadastro Único (Single Registry)**

This is a centralized system for managing social Programmes. It improves targeting and efficiency but raises concerns about data protection and potential misuse during elections. Weak legal frameworks for data privacy could allow political exploitation.[10]

- **South Korea: The Smart Cities**

Project uses DPI for integrated services like traffic management and public safety. Concerns include over-surveillance and inadequate citizen consent, particularly regarding facial recognition technologies used for monitoring public spaces.[11]

- **European Union: Digital ID Wallet**

Aims to provide secure access to services across member states. Although it adheres to strict GDPR standards, critics highlight risks of centralizing sensitive data and the challenges of ensuring cross-border cybersecurity and trust.[12]

- **United States: Federal Digital Identity Framework**

The U.S. government's National Institute of Standards and Technology (NIST) has developed a framework for secure digital identities. However, adoption remains fragmented across states, reflecting broader debates over federal versus state control in digital governance, and there are concerns about corporate involvement leading to potential misuse of personal data.[13] This division highlights challenges in establishing unified regulatory standards and protocols, as states often assert autonomy over digital infrastructure and privacy frameworks, leading to inconsistencies in implementation. Additionally, the involvement of private corporations in managing digital identity systems raises concerns about potential misuse of personal data, particularly in jurisdictions lacking robust oversight mechanisms. These dynamics underscore the tension between creating a cohesive national framework and respecting state-level authority, which complicates efforts to ensure both security and privacy in digital governance.

- **Australia: My Health Record System**

This is Australia's centralized electronic health records aim to improve healthcare access and efficiency. Public backlash over automatic enrollment without robust consent mechanisms led to revisions. Concerns persist regarding data security and the system's vulnerability to breaches.[14]

- **Singapore: National Digital Identity (NDI)**

This enables seamless access to public and private services using a single digital identity. Despite its efficiency, critics argue that strong state control over data could suppress dissent or invade privacy if not adequately safeguarded.[15]

---

10 https://documents1.worldbank.org/curated/en/972261468231296002/pdf/398530SP1709.pdf

11 https://documents1.worldbank.org/curated/en/099501509212220541/pdf/IDU09bc4586900d9a047080a9de0afa91af324a9.pdf

12 https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Security+and+Privacy

13 https://itif.org/publications/2024/09/23/path-to-digital-identity-in-the-united-states/

14 https://www.anao.gov.au/work/performance-audit/implementation-the-my-health-record-system

15 https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-importance-of-a-national-digital-identity-system

3. Regional Case Studies of DPI

The African Union's Digital Transformation Strategy (2020–2030) seeks to harmonize DPI across member states to foster regional integration, e-commerce, and governance.[16] However, disparities in infrastructure, digital literacy, and regulatory frameworks between countries pose significant challenges. Efforts like Smart Africa's Single Digital Market aim to address these disparities by promoting interoperability and inclusivity.

- **Tanzania: National ID System (NIDA)** oversees the country's biometric national ID Programme, launched to improve service delivery and enhance financial inclusion. The system integrates with various services, such as banking and mobile money platforms. However, concerns have arisen about data security and exclusion, particularly for marginalized groups like pastoralists and women in rural areas, who face challenges in registration due to limited outreach and documentation requirements.[17]
  For pastoralist communities, these challenges are compounded by their nomadic lifestyles, which make it difficult to access registration centers and maintain the necessary paperwork. This exclusion risks deepening their marginalization, as they are unable to access essential services like banking, healthcare, or mobile money, further entrenching cycles of poverty and social inequality.

  The system integrates with various services, such as banking and mobile money platforms. However, concerns have arisen about data security and exclusion, particularly for marginalized groups like pastoralists and women in rural areas who face challenges in registration due to limited outreach and documentation requirements.[18]

- **Uganda:** Mobile Money Integration has integrated mobile money platforms with government services, enabling citizens to pay taxes, access social benefits, and conduct financial transactions digitally. While this enhances efficiency, it raises issues of digital equity, as rural populations and women are less likely to own mobile phones or access the internet. Additionally, the government's surveillance capabilities and the imposition of social media and mobile money taxes have raised privacy and affordability concerns.[19]

- **Rwanda:** Irembo e-Government Platform serves as a centralized portal for accessing government services online, including birth registration, passport applications, and business permits. The initiative is lauded for its efficiency and accessibility for urban residents but criticized for leaving rural communities behind due to inadequate digital literacy and infrastructure. Efforts are ongoing to bridge this gap, but challenges remain in ensuring universal accessibility.[20]

- **South Africa: The Biometric Social Grant System,** implemented through the South African Social Security Agency (SASSA), facilitates the distribution of social grants to millions of citizens. While it reduces fraud and improves efficiency, the system has faced backlash over privacy breaches and allegations of unlawful data sharing with private corporations.

16 https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf
17 https://researchictafrica.net/2 021/07/16/tanzania-nida-ids-for-civic-services-or-not/
18 https://researchictafrica.net/2021/07/16/tanzania-nida-ids-for-civic-services-or-not/
19 https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/09/GSMA-EUE-FINAL.pdf
20 https://dial.global/wp-content/uploads/2024/08/rwanda-final.pdf

The lack of informed consent and transparency in data usage has sparked legal and civil society interventions.[21] Notably, the South African Constitutional Court ruled against Net1, the parent company of the grant payment provider CPS, for its improper handling of grant beneficiaries' data without explicit consent, setting a legal precedent for safeguarding personal information.

Additionally, the Protection of Personal Information Act (POPIA) has been invoked to strengthen privacy protections, mandating stricter controls over data sharing and ensuring that SASSA and its contractors comply with data protection principles. These interventions highlight the growing legal scrutiny over biometric data governance and the need for robust accountability frameworks. While it reduces fraud and improves efficiency, the system has faced backlash over privacy breaches and allegations of unlawful data sharing with private corporations. The lack of informed consent and transparency in data usage has sparked legal and civil society interventions.[22]

- **Nigeria:** Nigeria's National Identity Management Commission (NIMC) administers NIN a biometric digital ID system (Digital Identity Programme) aimed at streamlining access to government services and BVN a secure verification system for banking for fostering financial inclusion. Despite its potential, the programmes faces challenges, including digital exclusion exhibited through low enrolment rates, a lack of infrastructure in remote areas, and concerns about weak data protection framework which leave personal data vulnerable.[23] Nigeria's weak legal framework for data privacy exacerbates fears of misuse.[24]

- **Ethiopia:** Ethiopia recently launched a digital ID pilot Programme under its Digital Ethiopia 2025 strategy. The initiative aims to enhance access to services, financial inclusion, and governance. However, ethnic conflicts and political instability pose challenges to equitable deployment, raising fears of exclusion or misuse of personal data in politically sensitive regions.[25]

- **Ghana: National Digital Property Address System,** integrates digital addresses with identification data to improve service delivery and support e-commerce. The initiative aims to bridge gaps in formal property ownership and service delivery but faces hurdles in reaching rural areas and ensuring data security. Additionally, limited public awareness hinders adoption.[26]

These examples illustrate both the promise and the risks of DPI globally and regionally, highlighting the importance of adopting rights-based approaches to design and implementation.

21 https://chrgj.org/2021-03-11-locked-in-south-africa-welfare-state-digital-monopoly/
22 https://popia.co.za/category/data-subject/
23 Olanrewaju, A. (2022). "Digital Identity in Nigeria: Challenges and Lessons."
24 https://cipesa.org/wp-content/files/Ecosystem-Approach-to-Digital-Identification-Enrolment-Assessing-the-Opportunities-and-Risks-in-Nigeria-Report.pdf
25 https://www.weforum.org/stories/2024/03/bridging-the-digital-divide-challenges-and-opportunities-for-ethiopias-digital-transformation/
26 https://brickstone.africa/ghanas-digital-address-system-failure/

4. Global DPI Experiences and Human Rights Implications: An In-Depth Analysis

Digital Public Infrastructure (DPI) is emerging as a cornerstone of modern governance, transforming service delivery, enhancing inclusion, and fostering societal connectivity. However, the implementation of DPI often reveals a dual nature—its capacity to drive innovation is frequently accompanied by significant risks, including privacy infringements, surveillance, and systemic exclusion. This report examines global and African experiences with DPI, underscoring their opportunities, pitfalls, and human rights implications, with a particular focus on Kenya's evolving DPI landscape.

China's DPI landscape exemplifies how technology can be leveraged to enhance control and governance. The Social Credit System integrates digital identity, financial data, and behavioral metrics to rank citizens and businesses. While proponents hail it as a mechanism for promoting trustworthiness, critics view it as a surveillance tool that curtails personal freedoms. Individuals with low scores can face travel restrictions or denial of credit access. Additionally, China's widespread use of facial recognition technology, particularly in targeting ethnic minorities such as the Uyghurs, has raised alarm over human rights abuses, demonstrating the darker possibilities of unchecked DPI deployment.

India's Aadhaar system, the largest biometric identification initiative in the world, has successfully connected over 1.3 billion citizens to essential services. However, its deployment has not been without controversy. Cases of individuals being denied food rations due to authentication failures highlight the precarious line between inclusion and exclusion. Privacy concerns are equally pressing, with multiple instances of unauthorized access to the Aadhaar database. This underscores the risks of over-reliance on technology and the need for robust data protection laws. Estonia stands out as a global leader in e-governance, with its X-Road platform providing secure access to public services. Unlike many other systems, Estonia's infrastructure is designed with privacy in mind, employing blockchain technology to protect personal data. However, challenges remain, particularly in bridging the digital divide for rural and elderly populations. The Estonian experience highlights the importance of balancing innovation with inclusivity and user accessibility.

Brazil's adoption of electronic voting systems has streamlined electoral processes, increasing efficiency and transparency. Despite these advances, the system has faced cyberattacks and misinformation campaigns that question its integrity. The 2022 elections saw heightened political polarization, fueled by claims of vulnerabilities in the system. This case demonstrates the critical need for robust cybersecurity measures and public trust to safeguard democratic processes.
Ukraine's Diia app consolidates services like digital IDs, healthcare, and business licenses. It has been instrumental in enhancing accessibility and governance. However, the ongoing conflict with Russia exposes the vulnerabilities of such infrastructure. Cyberattacks have targeted sensitive personal data, raising concerns about the weaponization of information in conflict zones. The United States leverages DPI systems such as Social Security and healthcare databases to enhance service delivery. However, revelations of mass surveillance, such as the NSA's PRISM Programme, highlight the tension between national security and privacy rights. These concerns underline the necessity of transparent data governance frameworks to protect individual freedoms. During the COVID-19 pandemic, South Korea employed DPI for digital contact tracing and QR-code-based systems to mitigate virus spread. While effective in public health management, these measures sparked debates over data transparency and fears of entrenched surveillance beyond the pandemic's scope.

Tanzania's biometric ID Programme, managed by the National Identification Authority (NIDA), aims to streamline service access. Yet, documentation barriers have excluded significant portions of the population from vital services, including healthcare and banking. This mirrors similar challenges faced by Kenya's Huduma Namba initiative, underscoring the regional risks of exclusion inherent in poorly implemented DPI systems.

Nigeria mandates biometric SIM registration, citing national security concerns. However, the absence of stringent data protection laws has led to fears of data misuse and surveillance. Reports of leaked biometric data highlight the vulnerabilities of inadequately regulated DPI systems, emphasizing the urgent need for robust safeguards.

South Africa's digital payment system for social grants has enabled millions to access critical financial support. Nonetheless, cybersecurity breaches have left beneficiaries vulnerable to fraud and data theft. This highlights the need for resilient cybersecurity measures to protect sensitive information, particularly for marginalized populations.

Ghana's biometric National Identification System has improved financial inclusion by expanding access to banking services. However, delays in implementation and technical challenges have marginalized some communities. These issues highlight the importance of equitable and timely rollouts in DPI projects.

Ethiopia's digital ID initiative seeks to consolidate fragmented identity systems. Yet, political instability raises fears of ethnic profiling and misuse of personal data. The Ethiopian case underscores the heightened risks DPI poses in regions experiencing conflict and political turmoil. Uganda's adoption of biometric systems for voter registration and national ID cards has faced criticism for enabling state surveillance. Opposition leaders and activists have reported harassment linked to their digital footprints, illustrating how DPI can be weaponized in repressive regimes.

5. Kenya's DPI Landscape and Human Rights Issues

Kenya has emerged as a leader in adopting Digital Public Infrastructure (DPI) across Africa, leveraging technology to drive financial inclusion, enhance governance, and improve public service delivery. The country's DPI initiatives span digital identity systems, mobile payment platforms, open data initiatives, and smart city projects. However, significant human rights concerns, ethical issues, and implementation challenges persist despite these advancements. Below is a comprehensive exploration of Kenya's DPI landscape, detailing key initiatives, impacts, and associated challenges.

The country's financial DPI, led by MPESA, has driven financial inclusion but raised questions about data privacy and surveillance. Similarly, global projects like Worldcoin, which collected biometric data in Kenya, have highlighted the ethical dilemmas surrounding data commodification. These cases reflect the need for Kenya to adopt robust legal frameworks and inclusive implementation strategies to mitigate DPI risks while maximizing its benefits.

Huduma Namba and **Maisha Number:** introduced in 2019, aimed to integrate multiple government services into a unified digital ID system. However, the lack of a comprehensive data protection framework led to significant legal challenges. In 2021, the High Court halted its rollout, citing concerns over privacy, lack of public consultation, and the absence of clear safeguards

against misuse of personal data. This ruling marked a crucial moment in Kenya's digital governance, highlighting the importance of establishing strong legal and regulatory frameworks before implementing large-scale biometric systems.[27]

The current administration has proposed renaming **Huduma Namba** to **Maisha Number**, aiming to address past concerns, such as better data protection measures and improved inclusivity. Critics, however, argue that rebranding alone does not resolve systemic issues, such as data security vulnerabilities and the exclusion of marginalized communities. Looking ahead, the **Maisha Number** initiative has the potential to incorporate lessons learned from **Huduma Namba,** particularly in terms of ensuring privacy protections, transparency in data use, and broad public engagement to avoid repeating past mistakes in the digital identity space. However, the lack of a comprehensive data protection framework led to legal challenges, with the High Court halting its rollout in 2021.[28] The current administration has proposed renaming Huduma Namba to Maisha Number, aiming to address past concerns. However, critics argue that the rebranding does not resolve systemic issues in data security vulnerabilities and the exclusion of marginalized communities. Looking ahead, the Maisha Number initiative has the potential to incorporate lessons learned from Huduma Namba, particularly in terms of ensuring privacy protections, transparency in data use, and broad public engagement to avoid repeating past mistakes in the digital identity space.[29]

Worldcoin and Biometric Data Exploitation: Worldcoin's controversial rollout in Kenya exemplifies the risks of biometric data collection. Launched in 2022, the cryptocurrency project offered financial incentives in exchange for iris scans, leading to concerns about the exploitation of economically vulnerable communities who may not have fully understood the implications of sharing such sensitive data.

Critics argued that the lack of informed consent and the absence of adequate transparency in how the data would be used violated privacy principles. International best practices, such as those outlined in the EU's General Data Protection Regulation (GDPR), emphasize the importance of explicit informed consent, the minimization of data collection, and ensuring secure data storage and processing.[30] In response, the Kenyan government suspended Worldcoin in 2023, citing violations of the Data Protection Act (2019), which mandates strict safeguards for personal data and requires clear consent mechanisms.[31]

---

27 https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

28 Nubian Rights Forum & 2 Others V. AG. & 6 others; Child Welfare Society & 9 Others [Interested Parties] [2020] eKLR vailable at https://new.kenyalaw.org/akn/ke/judgment/kehc/2020/8772/eng@2020-01-30

29 https://www.kictanet.or.ke/maisha-namba-project-a-balancing-act-between-modernization-and-public-trust/

30 https://gdpr-info.eu/art-5-gdpr/https://www.ca.go.ke/ca-and-data-commissioner-warn-kenyans-over-worldcoin https://africanlegalstudies.blog/2023/09/22/lessons-from-kenyan-governments-response-to-world-coin-biometric-crypto-project/

31 https://documents1.worldbank.org/curated/pt/727791468337814878/585559324_201406191042051/additional/722360PUB0EPI00367926B9780821389911.pdf

The High Court of Kenya, in its ruling dated September 2023, upheld the suspension, emphasizing the need for strict adherence to the Data Protection Act.[32] The court raised concerns about the company's failure to demonstrate compliance with Kenyan data protection laws and highlighted the importance of ensuring foreign entities comply with local regulations regarding biometric data collection.[33] The ruling also reinforced the necessity of robust regulatory frameworks to prevent exploitation and ensure transparency in the processing of sensitive personal data, in line with international standards."

MPESA and Financial Data Privacy: Kenya's MPESA platform has revolutionized financial inclusion, allowing millions to access banking services and facilitating mobile money transactions. However, reports of data sharing with third parties and unauthorized surveillance have raised significant privacy concerns.[34]

To address these issues, MPESA could align more closely with GDPR-like standards, which emphasize transparency, data minimization, and user control over personal data. Under GDPR, users must be informed of how their data will be used and have the right to withdraw consent at any time. MPESA could enhance its privacy practices by adopting similar mechanisms, such as providing clearer consent options for users before sharing their data with third parties and ensuring that users are fully aware of how their transaction data is being utilized. Moreover, MPESA could implement stronger data protection measures to safeguard against unauthorized access or surveillance, including more rigorous encryption and anonymization techniques, in line with GDPR's requirements for data security.

Additionally, the platform's transaction fees, which disproportionately affect low-income users, have led to calls for more equitable pricing models. Aligning with GDPR's principle of fairness and transparency, MPESA could improve pricing structures by offering more affordable options for vulnerable groups and providing clear, upfront information about fees. Such adjustments could help ensure that financial inclusion is not only expanded but is also equitable, with a focus on both privacy protection and fair access to services. By adopting GDPR-like standards, MPESA would not only enhance user trust but could also set a benchmark for other mobile money platforms in emerging economies, fostering a more privacy-conscious and inclusive financial ecosystem."

eCitizen and the Digital Divide: The eCitizen portal centralizes access to government services but excludes citizens without internet access or digital literacy. System downtimes and cybersecurity vulnerabilities further hinder its effectiveness, demonstrating the importance of building resilient infrastructure.

IFMIS and Corruption Risks: The Integrated Financial Management Information System (IFMIS) aims to enhance public financial transparency. However, it has been implicated in high-profile corruption cases, such as the National Youth Service scandal, where system vulnerabilities were exploited for financial mismanagement.

---

[32] Nubian Rights Forum & 2 Others V. AG. & 6 others; Child Welfare Society & 9 Others [Interested Parties] [2020] eKLR vailable at https://new.kenyalaw.org/akn/ke/judgment/kehc/2020/8772/eng@2020-01-30

[33] https://africanlegalstudies.blog/2023/09/22/lessons-from-kenyan-governments-response-to-world-coin-biometric-crypto-project/

[34] https://documents1.worldbank.org/curated/pt/727791468337814878/585559324_20140619042051/additional/722360PUB0EPI00367926B9780821389911.pdf

Smart Cities and Surveillance: Kenya's Konza Technopolis project, aimed at fostering economic growth through smart city infrastructure, has raised concerns about mass surveillance and the exclusion of low-income citizens.

To address these issues, Kenya's Data Protection Act (2019) provides legal provisions that can mitigate the risks associated with surveillance technologies. The Act requires explicit consent from individuals before collecting personal data, ensures data minimization, and mandates that only necessary data is collected and retained.[35] It also stipulates that data processors implement strong security measures to protect personal data from misuse. Additionally, the Act grants individuals the right to access and correct their data, ensuring transparency in the use of surveillance systems. The Data Protection Commissioner can enforce compliance with these rules, and penalties can be imposed for non-compliance. By leveraging these provisions, the Konza Technopolis project can balance technological advancement with the protection of privacy, ensuring that surveillance practices align with legal standards and do not disproportionately affect marginalized communities. The deployment of DPI in Kenya and globally offers immense potential for progress but also poses significant risks to human rights. From China's mass surveillance to Kenya's Worldcoin controversy, the challenges of data privacy, exclusion, and misuse are evident. As nations like Kenya expand their DPI initiatives, robust regulatory frameworks, informed public participation, and transparent governance are essential to ensure these systems promote inclusivity, equity, and rights protection. Balancing technological advancement with human rights is not just a necessity—it is a moral imperative.

Recommendations for Strengthening DPI Globally and Regionally

To maximize the benefits of DPI while mitigating its risks, a comprehensive approach is necessary. These recommendations are tailored to address global and regional challenges and highlight best practices for inclusive, secure, and rights-respecting DPI development.

Global Recommendations

1. **Adopt Robust Legal and Regulatory Frameworks**

Governments should establish and enforce clear, comprehensive laws that govern data protection, privacy, and cybersecurity. These frameworks must comply with international human rights standards to ensure that DPI initiatives prioritize individual freedoms.

- Example: The European Union's General Data Protection Regulation (GDPR) sets a global benchmark by imposing strict data protection rules, ensuring transparency and accountability in data handling.

- Recommendation: Countries without such frameworks should adopt similar regulations tailored to their specific contexts, ensuring alignment with global best practices.

2. **Ensure Privacy by Design in DPI Systems**

DPI should be developed with privacy and security as fundamental design principles to minimize misuse risks. Employing technologies such as encryption, blockchain, and anonymization can enhance user protection.

[35] https://erepository.uonbi.ac.ke/handle/11295/164087

- Example: Estonia's X-Road platform demonstrates how DPI can prioritize privacy and resilience through secure data exchange and decentralized architecture.

- Recommendation: Governments must mandate the integration of privacy-enhancing technologies during the development phase of DPI projects.

3. **Promote Digital Inclusivity**

Efforts must focus on reducing the digital divide to ensure marginalized communities can access and benefit from DPI. This includes providing affordable internet, investing in digital literacy programs, and addressing barriers such as language and accessibility.

- Example: India's Aadhaar system highlights how DPI can promote financial inclusion but also underscores the risks of exclusion due to technical failures or lack of digital literacy.

- Recommendation: Governments must conduct baseline assessments to identify and address the needs of underrepresented groups before rolling out DPI.

4. **Strengthen Cybersecurity**

DPI systems are attractive targets for cyberattacks, especially during conflicts or political instability. A global coalition to share best practices, intelligence, and resources can enhance collective cybersecurity.

- Example: Ukraine's Diia app underscores the importance of securing DPI during crises, as personal data can become a weapon of war.

- Recommendation: Governments should establish centralized cybersecurity agencies and conduct regular stress tests to assess vulnerabilities in DPI systems.

5. **Foster International Collaboration**

DPI initiatives often involve multinational corporations and cross-border data flows. Global cooperation is essential to harmonize standards, prevent exploitation, and ensure that DPI fosters collective growth. Existing frameworks like the Budapest Convention on Cybercrime provide useful models for international collaboration in cybersecurity. The Convention emphasizes cooperation among nations in the investigation and prosecution of cybercrime, setting standards for data protection and cross-border data sharing.[36] Adapting similar frameworks for DPI cybersecurity could help ensure consistent protection of digital infrastructure, reduce vulnerabilities, and foster trust among international stakeholders.

- Recommendation: International bodies such as the United Nations should play a central role in developing DPI governance standards that respect human rights and facilitate equitable access.

[36] Budapest Convention, available at < https://rm.coe.int/prems-105223-gbr-2023-convention-cybercrimi-ninalite-a5-web-4-/1680ae7118>

Regional Recommendation: The Africa Context

Gender Dynamics: Many African nations face significant gendered barriers in accessing DPI systems, particularly in rural areas. Women often encounter challenges such as limited access to technology, lower digital literacy, and socio-cultural factors that hinder their full participation in the digital economy.

A context-specific legal framework is needed to address these gender disparities, ensuring that DPI initiatives are inclusive and equitable. For example, countries can look to the Malabo Convention as a foundation for establishing laws that promote gender-sensitive digital policies, ensuring women have equal access to digital services and protecting them from potential data privacy breaches.

Impact of Political Instability: Political instability in many African countries such as Ethiopia has disrupted the implementation of DPI systems by destabilizing governance structures and hindering the establishment of reliable digital infrastructure. Legal frameworks must take into account the impact of political volatility on digital initiatives. Context-specific legal protections, like those outlined in the Malabo Convention, should focus on creating resilient digital frameworks that can withstand periods of political instability. By establishing clear guidelines for DPI in times of crisis, these frameworks would help maintain continuity, ensure data security, and preserve public trust in digital systems.

Private Sector Accountability: The private sector, particularly multinational corporations, plays a pivotal role in DPI but must be held accountable for protecting user data and respecting privacy. As demonstrated by concerns over platforms like M-Pesa, multinational corporations often operate in regions with weaker regulatory frameworks, putting consumers at risk of data misuse.

To address this, countries should develop tailored legal frameworks that draw on the Malabo Convention, ensuring that multinational companies operating in their territories are required to comply with strong data protection standards. This would foster accountability, encourage transparency, and safeguard the privacy of vulnerable populations, particularly in regions with limited regulatory oversight.

Data Protection Authorities: Data Protection Authorities (DPAs) play a central role in overseeing DPI systems and ensuring that citizens' digital rights are respected. However, in many African countries, DPAs lack the capacity, resources, or independence to effectively enforce data protection laws. To address this, countries should build on regional frameworks like the Malabo Convention, which encourages the establishment of strong, independent DPAs. These authorities must be equipped with the necessary tools to enforce data privacy regulations and protect citizens from abuses by both governments and corporations. Strengthening DPAs and empowering them to act decisively will ensure that DPI systems operate in a manner that respects citizens' rights and complies with established data protection standards.

Judicial Oversight: The judiciary has a critical role in overseeing DPI systems, especially in adjudicating cases related to data privacy violations, data breaches, and exclusion. To ensure that judicial oversight is effective, countries should adopt legal frameworks inspired by the Malabo Convention that provide clear guidelines for the judiciary in handling digital rights cases. By strengthening judicial oversight in DPI, courts can safeguard citizens' rights, ensuring that DPI initiatives operate within constitutional and legal boundaries. These frameworks can offer courts the necessary legal backing to challenge abuses and hold entities accountable for violations of privacy and data security.

6. **Address Documentation Barriers in Digital ID Systems**

A common issue across African DPI initiatives, including Tanzania's NIDA and Kenya's Huduma Namba, is the exclusion of individuals who lack the required documentation. This often affects marginalized communities, such as pastoralists, those in rural areas, and people living in informal settlements, who may not have access to formal identity documents. This exclusion undermines the inclusivity of digital ID systems, preventing individuals from accessing essential services such as banking, healthcare, and government aid.

- Recommendation: Governments should develop flexible and inclusive registration processes that can accommodate people who lack formal documentation. One promising approach is community-based verification, which allows trusted local authorities or community members to vouch for individuals' identities. A successful example of this approach is Rwanda's Irembo platform, which has adopted flexible registration methods, enabling citizens to use community-based verification to access government services without the need for formal documents. By leveraging local knowledge and community trust, this system ensures that no one is left behind due to bureaucratic barriers. This approach can be adapted and scaled to other countries across Africa, including Tanzania and Kenya, to ensure that marginalized groups are included in national digital identity systems. Such inclusive processes would promote equitable access to services and foster greater participation in the digital economy.

7. **Enhance Digital Literacy and Infrastructure**

Limited digital literacy and infrastructure disparities hinder the success of DPI across Africa. Investments in education and infrastructure are critical.

- Example: Ghana's delays in implementing its biometric National Identification System highlight the need for technical and logistical capacity building.

- Recommendation: Governments should prioritize public awareness campaigns and establish digital skills training programs, especially for rural populations.

8. **Mitigate Surveillance Risks in Repressive Contexts**

DPI in authoritarian regimes, such as Uganda's biometric voter registration system, often enables state surveillance and political harassment.

- Recommendation: Civil society organizations and regional bodies must advocate for safeguards to prevent DPI misuse, such as independent oversight bodies and whistle-blower protections.

9. **Secure DPI against Cyber Threats**

African nations are increasingly becoming targets of cyberattacks, with incidents such as the breaches in South Africa's social grant system highlighting the vulnerabilities in digital infrastructure. These attacks not only undermine trust in digital services but also compromise the security of personal data, putting citizens at risk. Strengthening cybersecurity is thus critical to ensuring the integrity and safety of Digital Public Infrastructure (DPI) systems.

- Recommendation: Governments should establish public-private cyber defense task forces at both the global and regional levels to pool expertise and resources in addressing cyber threats. For instance, an AU-led cybersecurity task force could be created to focus on strengthening the security of DPI systems across African nations. Such a task force would bring together governments, private sector experts, and international organizations to share best practices, coordinate responses to cyber threats, and develop common standards for securing digital infrastructure. By leveraging the combined expertise of both public and private sectors, African countries can create more resilient digital systems that are better equipped to defend against evolving cyber risks. This collaborative approach would also enable African nations to better respond to emerging cybersecurity challenges and ensure that the continent's digital economy can thrive safely.

10. **Encourage Public-Private Partnerships (PPPs)**

DPI development often requires significant resources, which can be supplemented through PPPs. However, these partnerships must prioritize public welfare over profit.

- Example: Kenya's MPESA is a testament to the transformative potential of PPPs in driving financial inclusion.

- Recommendation: Governments must establish clear accountability mechanisms to ensure private sector involvement does not compromise public interests.

11. **Promote Regional Knowledge Sharing**

African nations can benefit from sharing experiences, lessons, and innovations in DPI implementation.

- Example: Regional hubs, such as the Smart Africa Initiative, facilitate dialogue and collaboration on digital transformation projects.

- Recommendation: Countries should actively participate in such initiatives, focusing on scalable and replicable solutions.

The Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ICJ Kenya House, Off Silanga Road, Karen
P.O. Box 59743 - 00200, Nairobi, Kenya
www.icj-kenya.org

ICJ Kenya