Strathmore University
Centre for Intellectual Property and Information Technology Law

A Report on the Study of Government Digital Services and Digital ID in Kenya and Zambia

Under the Project:
Advancing the Governance of Data for Development in Africa: Strengthening Regional Integration and National Capacity in the Provision of Government Digital Services

ACKNOWLEDGMENT

The preparation and publication of this report have been made possible through funding from the **International Development Research Centre (IDRC)**. We extend our appreciation to **Dr Melissa Omino**, the Director, whose vision and guidance were central to the development of this report.

We acknowledge the primary authors, **Dr Nelly C Rotich** and **Joshua Kitili** for their commitment and expertise. Thank you to **Calvin Mulindwa**, **Doreen Aoko Abiero**, **Josephine Kaaniru** and **Irene Musengya Makau** for their valuable contributions to the report's content. We are grateful to **Mr Mustafa Mahmoud** for facilitating the collection of surveys that informed the analysis.

Finally, we recognise the **administrative team** at **CIPIT** for their support throughout the process of developing this report.

TABLE OF CONTENTS

Image Source: vecteezy.com

ACRONYMS & ABBREVIATIONS

CSO	Civil Society Organisation
DPA	Data Protection Act
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DZAP	Digital Zambia Acceleration Project
eKYC	Electronic Know Your Customer
eNRC	Electronic National Registration Card
ICT	Information and Communications Technology
ID	Identification
INRIS	Integrated National Registration Information System
IPRS	Integrated Population Registration System
KRA	Kenya Revenue Authority
KYC	Know Your Customer
NRB	National Registration Bureau
NRC	National Registration Card
NSSF	National Social Security Fund
NTSA	National Transport and Safety Authority
SHA	Social Health Authority

Image Source: vecteezy.com

EXECUTIVE SUMMARY

This report examines the landscape of government digital services and digital identity systems in Kenya and Zambia, with a focus on responsible and rights-preserving data systems. As governments across Africa move services to digital platforms, this shift holds great promise for improving access, efficiency, and inclusion. However, it also introduces a complex set of challenges related to data privacy, legal protections, exclusion, and institutional capacity. Thus, this research provides a detailed examination of the structures, policies, and stakeholder dynamics shaping digital ID and government digital services in Kenya and Zambia.

The research aimed to identify governance frameworks and implementation strategies for digital ID and government digital services, assess institutional and regulatory gaps, and propose strategies for collaborative engagement among governments, civil society organisations (CSOs), and private sector actors. The study employed a mixed-methods approach, including an extensive literature review, legal analysis, and stakeholder surveys targeting CSOs, government agencies, and private companies. While the research achieved broad engagement in Kenya, it encountered limited participation from government and private sector stakeholders in Zambia, reflecting institutional hesitation around digital identity issues.

Findings reveal that both Kenya and Zambia have made significant investments in digital ID and digital government services. Kenya has introduced Maisha Namba, eCitizen, and Huduma Kenya Service Delivery Programme. Zambia is deploying biometric IDs through its Integrated National Registration Information System (INRIS) and electronic National Registration Cards (eNRC), while also expanding rural access via the Smart Village and Digital Zambia Acceleration Project. These efforts are supported by foreign donors and technology providers, including the World Bank, Huawei, and the Bill & Melinda Gates Foundation. However, in both countries, reliance on external partners raises concerns around data sovereignty and long-term sustainability.

Despite existing legal frameworks, such as Kenya's Data Protection Act of 2019 and Zambia's Data Protection Act of 2021, enforcement remains weak. Regulatory bodies lack sufficient resources, technical capacity, and autonomy, undermining the effective protection of personal data. Moreover, the legislative environment has not adequately addressed the risks posed by overcollection of biometric data, opaque data-sharing practices, or the lack of informed consent. These challenges are particularly acute for marginalised communities, such as the Nubian community in Kenya, refugees, women, and rural populations, who often face discriminatory vetting procedures, poor access to documentation, or limited digital literacy.

CSOs play a critical role in addressing these gaps. They are engaged in legal empowerment, policy advocacy, public awareness campaigns, and digital rights training, helping communities navigate complex identification systems and hold institutions accountable. The private sector, while instrumental in deploying infrastructure and services, has called for clearer regulatory guidance and improved collaboration with oversight agencies. Government stakeholders acknowledge challenges related to data security, capacity gaps, and service delivery inefficiencies, particularly in rural areas.

In response to these findings, the report recommends comprehensive legislative reform to close regulatory gaps and align national laws with global data protection standards. It also calls for investment in cybersecurity, inclusive digital access strategies, and sustained capacity-building across all sectors. Strengthening inter-agency coordination, promoting ethical digital technologies, and establishing mechanisms for citizen feedback and redress are essential to creating transparent, inclusive, and accountable digital governance systems.

The report underscores that while digital ID systems and government digital services hold transformative potential, they must be developed with attention to justice, inclusion, and rights. Building trustworthy, rights-preserving digital infrastructures requires not only technical and financial investments, but also participatory governance and a commitment to protecting the most vulnerable. This study offers a roadmap for policymakers, civil society, and development partners to ensure that Africa's digital transformation delivers equitable and meaningful benefits for all.

PART ONE

INTRODUCTION

1.1 Introduction to the Study

African governments transitioning citizen services, including voter registration and state benefits, into digital formats also helps expand access to human rights, fostering democratic engagement, and enhancing the efficiency of government services and administration. This move towards digitalisation is in harmony with the implementation of fundamental digital or bio-ID systems, concurrently addressing the personal identification gap in Africa and providing formal identification to an estimated 500 million individuals presently without it. It also aligns with the objectives of Sustainable Development Goal 16.9 (universal legal identity) and the African Digital Transformation Strategy.

However, the digitalisation of government services introduces new challenges. These include cybersecurity and data privacy concerns arising from increased collection and centralisation of sensitive personal information, the need for policy and legal framework adjustments, potential risks to vulnerable communities, and the possibility of job loss due to automation. Like many other African countries, Kenya and Zambia also experience these challenges.

The digitalisation of government services in Kenya and Zambia necessitates rights-preserving data governance frameworks. These frameworks support responsible data collection, ethical use and transfer, and ensuring equitable and just realisation of data value. While government digital services data is valuable for addressing social challenges and developing solutions, it also contains sensitive personal information, necessitating stringent regulatory measures to protect vulnerable groups.

Recently, foreign entities have sought African data, highlighting concerns about data extraction, data colonialism, and the need for frameworks governing cross-border data sharing and data sovereignty. The lack of such frameworks poses challenges to utilising data's potential value for addressing social issues and growing the economy.

In February 2022, the African Union Commission published the African Union Data Policy Framework (DPF), aiming to establish and govern robust data systems. The DPF emphasises principles such as building trusted data environments, promoting cooperation between countries, ensuring fair and inclusive data systems, and empowering African governments for public good. It also highlights regulatory and capacity gaps that need attention.

To address these gaps, this research proposed a framework to advance responsible and rights-preserving data systems for digital government services in Kenya and Zambia. The research focused on generating evidence to support stronger regulation and policy, building capacity across government, civil society, and private institutions in Kenya and Zambia, and examining risks and opportunities for specific groups, including marginalised communities. Thus, relevant stakeholders in government, private sector, and civil society organisations in Kenya and Zambia were surveyed to identify challenges related to implementing existing frameworks and optimising capacity development by creating an enabling environment. This research has also conducted an extensive mapping of governance structures and implementation strategies for national digital ID services and national biographical data in Kenya and Zambia. The findings from the surveys inform the analyses in this report.

1.2 Objectives of the Study

The primary objective of this study was undertaking rigorous research on the rights-related data risks and governance requirements in the provision of government digital services and digital ID in Kenya and Zambia. The study was guided by these specific objectives:

i. Mapping the governance structures and implementation strategies for national digital ID services and national biographical data in Kenya and Zambia.

ii. Surveying institutional partners in Kenya and Zambia to understand institutional and organisational challenges in the governance of digital services data/biometric ID data.

iii. Surveying institutional partners in Kenya and Zambia to understand challenges impacting the implementation of existing frameworks on government digital services.

iv. Identifying ways through which governments, private organisations, civil society, and advocacy practitioners in Kenya and Zambia can effectively aid each other in leveraging the delivery of government digital services to the benefit of all.

1.3 Research Questions

The overarching research question is: *What governance design and implementation mechanisms are needed to address the existing regulatory, institutional and capacity gaps that inhibit the establishment of democratic, just and rights-preserving data systems in the provision of government digital services and digital ID in Kenya and Zambia?*

The specific research questions for this study's activities are:

i. What is the landscape of governance structures and implementation strategies for government digital services and national biographical data in Kenya and Zambia?

ii. What are the institutional and organisational challenges in the governance of digital services' data and biometric ID data in Kenya and Zambia?

iii. What are the challenges impacting the implementation of existing frameworks on government digital services in Kenya and Zambia?

iv. How can governments, private organisations, civil society, and advocacy practitioners in Kenya and Zambia effectively aid each other in delivering government digital services to the benefit of all?

1.4 Research Methodology

This study explored governance and data protection concerns arising from the implementation of government digital services and digital ID in Kenya and Zambia. This was done through a mixed-method research approach that combined both primary and secondary research. Primary data collection involved surveys of representatives from the government, civil society organisations and the private sector in Kenya and Zambia to understand institutional and organisational challenges in the governance of digital services data and biometric ID data. 10 CSOs, 10 government and five private sector organisations in Kenya and 10 CSOs in Zambia were surveyed.

Secondary data sources included a review of relevant academic literature, digital ID and national digital services reports, national digital services platforms, legal and policy frameworks and African and global initiatives on government digital services to understand the historical context and current developments of government digital services and digital ID. The research was also supplemented by the mapping of government digital services in Kenya and Zambia. In addition, this study conducted a rigorous examination of the power matrix in

the gendered impact of proposed and deployed digital government services and digital biometric ID requirements. This included an analysis of the existing and upcoming policy, the role of foreign companies and States, the effect of skewed knowledge structures and the systemic inequalities that digital national service platforms may perpetuate or exacerbate. Some of the outputs from this study have been and will be published in the form of blog articles and podcasts accessible on the CIPIT website. Collectively, the outputs in this study inspire the findings in this report.

1.5 Scope and Limitations of the Study

At the proposal stage of this study, there were plans to conduct relevant research in four countries across the African region. Due to limited funding allocated to the project, the scope was narrowed down to two countries, where Kenya and Zambia were ultimately selected. The selection of these countries was informed by detailed discussions with the larger consortium of partners conducting research under this project. The essence was to increase collaboration and for better output. In addition, both Kenya and Zambia had an established government digital services regime. Both countries represent two regions in Africa: Eastern and Southern Africa.

During surveys, all the contacted participants in Kenya responded. In Zambia there were also plans to survey 10 CSOs, five government and five private sector organisations. However, the researchers only succeeded in obtaining feedback from CSO participants. Several challenges impacted the response timelines in Zambia, particularly by government and private sector participants. Government institutions in Zambia were reluctant to share information related to digital government services and digital IDs, and private sector participants did not provide responses. As a result, the surveys concluded without feedback from government and private sector participants in Zambia.


Image Source: vecteezy.com

Image Source: vecteezy.com

PART TWO

GOVERNANCE STRUCTURES AND IMPLEMENTATION STRATEGIES FOR GOVERNMENT DIGITAL SERVICES AND NATIONAL BIOGRAPHICAL DATA IN KENYA AND ZAMBIA

2.1 Introduction

Over the last few decades, digital technology has become indispensable for administrative running, both in the private and public sectors on a national, regional and global level. Globally, a surge in digital technologies, mobile phone use and internet connectivity has spearheaded a digital revolution, but unequal access, data protection challenges and other critical issues threaten to leave many behind.[1] This creates a digital divide exhibited by the gap between individuals and communities with access to and the use of digital technologies, and those who lack it.[2] Unequal access to new information communications technologies stemming from race, gender, territorial location or social class has resulted in a new form of social inequality.[3]

In response, governments are utilising universal access and universal service as key strategies to bridge the digital divide both within their countries and with the rest of the world.[4] Universal access enables every person to have access to necessary Information and Communications Technology (ICT) within a given distance for enhanced communication.[5] However, the difficulty is that individual countries employ different measures to determine adequacy. Universal service, on the other hand, relates to the logistical aspects of accessibility and entails the development of ICT that, in addition to being accessed by all, is capable of being used by all people irrespective of their physical (dis)abilities.[6]

Disparities in digital access are particularly pronounced in Africa. However, while the digital divide hinders the full embrace of digitisation, the potential benefits are vast, outweighing the adverse effects of ignoring the digital revolution. Given that 500 million Africans lack a birth certificate or other official identification, using digital forms of identification has increased in popularity to ease and reduce identity management costs.[7] As more services and opportunities such as banking, education and healthcare move online, digital identity becomes crucial for participation in the digital economy.[8]

Countries are racing to digitise their services. For example, the 50-IN-5 coalition of countries aims to transform their services to digital in five years, from 2023 to 2028, with countries coming together to commit to sharing learnings, best practices, and technologies that can ultimately reduce costs, build local capacity, maximise impact, and help radically shorten the implementation journeys for digital public infrastructure (DPI).[9] But what is DPI and how does it link to digital identity in both Kenya and Zambia?

The Universal DPI Safeguards Framework broadly defines DPI as "a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and/or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms".[10]

At the core of DPI lies Electronic Know Your Customer (eKYC) that is linked to a functional digital ID and digital registers that enable eKYC. It is therefore important to get it right at the ID level to ensure that DPI regimes are inclusive and do not

1 Bianca Reisdorf and Colin Rhinesmith, 'Digital inclusion as a core component of social inclusion' (2020) 8(2) Social Inclusion, 132 accessed 4 April 2024.

2 Sophie Lythreatis, Sanjay Kumar Singh, and Abdul-Nasser El-Kassar, 'The Digital Divide: A Review and Future Research Agenda' (2022) 175 Technological Forecasting and Social Change, 121359 accessed 7 April 2024.

3 Jan Van Dijk, 'Digital divide: Impact of access' (2017) The International Encyclopedia of Media Effects,1 accessed 15 April 2024.

4 Leanne Townsend, Arjuna Sathiaseelan, Gorry Fairhurst, and Claire Wallace, 'Enhanced Broadband Access as a Solution to the Social and Economic Problems of the Rural Digital Divide' (2013) 28(6) Local Economy, 580 accessed 5 April 2024.

5 Vassilis Koutkias, Vassilis, Nick Kaklanis, Konstantinos Votis, Dimitrios Tzovaras, and Nicos Maglaveras, 'An Integrated Semantic Framework Supporting Universal Accessibility to ICT' (2016) 15 Universal Access in the Information Society, 49 accessed 4 April 2024.

6 ibid.

7 Grace Mutung'u, 'Digital Identity in Kenya' (2021) <https://researchictafrica.net/wp/wp-content/uploads/2021/11/Kenya_1.11.21.pdf> accessed April 4 2024.

8 World Bank Group, 'World Development Report 2016: Digital Dividends' (World Bank Publications, 2016)

9 50in5, 'About' <https://50in5.net/#about> accessed 10 July 2025.

10 UN OSET and UNDP 2024, The Universal Digital Public Infrastructure Safeguards Framework,

leave anyone behind. This has led to several digital ID regimes in Kenya beginning with Huduma Namba in 2019, then Maisha Namba in 2023. Digital identity systems are crucial for transitioning to DPI with Kenya and Zambia actively transitioning from traditional methods to digital frameworks. Kenya's historical identity system, originating from the colonial "kipande" and evolving through various forms, has now modernised with the Maisha Namba initiative.[11] This initiative provides a Unique Personal Identifier (UPI) for citizens from birth to death, integrated with a digital platform that includes a third-generation ID card and a national population register. Maisha Namba is the foundation of Kenya's DPI. When issued at birth, the 14-digit UPI replaces the birth entry number that would previously have been captured at birth. For those seeking to replace their previous generation IDs, the 14-digit Maisha Namba and card replaces the old 8-digit ID number. Maisha Namba is then integrated with the population register that replaces the Integrated Population Registration System (IPRS) database. Lastly, Maisha Namba's digital ID counterpart is then used for online verification under eCitizen.[12]

In Zambia, the transition to digital identity began with the 2014-2019 National Strategic Action Plan promoting birth registration and certificate issuance.[13] The introduction of the electronic National Registration Card (eNRC) marks a significant modernisation step, although challenges such as gender disparities and societal norms affecting eNRC access and usage persist.[14]

Kenya and Zambia are actively developing their digital identity infrastructures, with substantial support from international partners, to improve access to services and enhance security. The Bill & Melinda Gates Foundation, for instance, committed significant funding towards these initiatives. In 2022, the foundation pledged $200 million to support digital public infrastructure globally, including digital IDs and civil registry databases.[15] This investment is aligned with the UN's Sustainable Development Goals, particularly the goal of achieving universal legal identity by 2030.

The United Nations Economic Commission for Africa (UNECA) is also instrumental in promoting digital ID systems in Africa, including in Kenya. UNECA's initiatives aim to create a roadmap for African governments to implement digital ID systems that support sustainable development and inclusive economic growth.[16] This involves collaboration with various stakeholders, including foreign companies and international organisations, to ensure the successful deployment and operation of these systems.

In both Kenya and Zambia, foreign entities and public-private partnerships are crucial in shaping the digital identity landscape. While these international collaborations bring necessary resources and expertise, it is vital that they prioritise local needs and sustainability. By leveraging digital technologies inclusively and fostering collaborative stakeholder engagement, both countries can develop more equitable and secure digital identity systems. These systems are intended to support socio-economic empowerment for all citizens, ensuring that the benefits of digital identity reach everyone.

11 Chris Burt, 'Kenya Signs Digital ID Support Deal with UNDP, Introduces a New Namba | Biometric Update' (www.biometricupdate.com14 August 2023) <https://www.biometricupdate.com/202308/kenya-signs-digital-id-support-deal-with-undp-introduces-a-new-namba> accessed 12 June 2024.

12 Aratek, 'The New Kenyan ID Card: Maisha Namba Explained' <https://www.aratek.co/news/the-new-kenyan-id-card-maisha-namba-explained> accessed 10 July 2025.

13 Calum Handforth and Matthew Wilson, 'Digital Identity Country Profile: Zambia' (2019) <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Zambia.pdf >accessed 12 June 2024.

14 ibid.

15 Chris Burt, 'Gates Foundation commits $200M to digital ID and other public infrastructure' (Biometric Update.com, 22 September 2022<Gates Foundation commits $200M to digital ID and other public infrastructure | Biometric Update> accessed 22 May 2024.

16 United Nations Economic Commission for Africa. <Implementing digital ID systems in Africa: ECA's Stakeholders Dialogue explores pathways for leveraging Digital ID Systems and disruptive technologies | United Nations Economic Commission for Africa (uneca.org)> accessed 22 May 2024.

2.2 Contextual Analysis of Government Digital Services and Digital ID in Kenya

Kenya, the third-largest economy in Sub-Saharan Africa, is leading in the adoption of the fourth industrial revolution: the digital economy. Kenya's digital economy is anchored on five pillars: digital infrastructure, digital business, innovation-driven entrepreneurship, digital skills and values, and digital government.[17] The digital infrastructure pillar enables the provision of affordable, accessible and reliable digital services. The digital government pillar focuses on the use of ICT for efficient, transparent and inclusive government services while the digital business pillar guides the development of a robust digital market supported by digital financial services. The innovation-driven entrepreneurship pillar offers innovations that are essential for the digital economy in the region in the provision of essential citizen services, social protection services, health, energy, digital learning, tax administration, judiciary, and land services, among others.[18]

The Kenya Service Delivery Programme, initiated in 2014 as a key component of the Kenya Vision 2030 Flagship project,[19] strives to revolutionise public service delivery. It focuses on ensuring that citizens have access to efficient, effective, and centred platforms through comprehensive one-stop-shop facilities.[20] This initiative is designed to streamline the interaction between the public and various government services, improving overall service efficiency and effectiveness while prioritising the needs and convenience of citizens. Significant digital government services and digital ID initiatives in line with this programme and Kenya's Vision 2030 are discussed in detail below.

2.2.1 Digital ID in Kenya

The introduction of the National Integrated Identity Management System (NIIMS) and the Huduma Namba was a testament to Kenya's commitment to creating a more efficient and user-friendly framework for accessing government services and ensuring every citizen has a unique personal identification number.[21] However, the implementation of the Huduma Namba faced criticism, and CSOs were excluded from the design and implementation phases.[22] There was also inadequate communication regarding its benefits.[23] For instance, the High court in case of *Nubian Rights Forum and 2 Others v Attorney General and 6 Others*[24] determined that the collection of DNA and GPS data for the NIIMS database was unjustified. This was all caused by the amendment of the registration of persons act to include DNA and GPS as part of biometrics. There was also scarce information about the system with the only information available being the compulsion for registration and deadlines.

The Kenyan Government announced its intention to replace the Huduma Namba cards with a new UPI number termed Maisha Namba.[25] The decision was made as part of an effort to distance the new system from the shortcomings associated with the Huduma Namba. Unlike the Huduma Namba, Maisha Namba registers births and deaths and functions as a digital ID for accessing various government services through the e-citizen digital platform.[26] This includes services provided by the Kenya Revenue Authority (KRA), the National Social Security Fund (NSSF), and the Social Health Authority (SHA). The UPI, assigned under the Maisha Namba, serves as

17 Meru, Abel Kinoti, and Mary Wanjiru Kinoti. "Digitalisation and public sector service delivery in Kenya." In Digital Service Delivery in Africa: Platforms and Practices, pp. 229-248. Cham: Springer International Publishing, 2022 accessed 12 June 2024.

18 Mkalama, Ben, Giacomo Ciambotti, and Bitange Ndemo. "Digital adoption in micro and small enterprise clusters: a dependency theory study in Kenya." In Handbook of Digital Entrepreneurship, pp. 199-220. Edward Elgar Publishing, 2022 accessed May 2024.

19 Kenya Gazette Notice No. 2177 of 4th April 2014 eKLR accessed May 2024.

20 Huduma Kenya, <https://www.hudumakenya.go.ke/aboutus> accessed 24 May 2024.

21 NIMS <NIMS - NIIMS, National Integrated Identity Management System - Nims> accessed on 29 April 2024.

22 Musoni M, Domingo E and Ogah E, 'Digital ID systems in Africa: Challenges, risks and opportunities', 2023, 23 accessed 14 May 2024.

23 ibid, 23.

24 Nubian Rights Forum and 2 Others v Attorney General and 6 Others, [2020] eKLR.

25 Wanga S, 'Kenyans to receive Maisha cards from November 1' The Standard November 2023, <Kenyans to receive Maisha cards from November 1 - The Standard (standardmedia.co.ke)> accessed on 22 April 2024.

26 Musoni M, Domingo E and Ogah E (n 22) 24 accessed 21 May 2024.

a foundational ID system with a centralised database that connects to functional ID systems, linked to a National Master Population Register (formerly the IPRS) to harmonise and consolidate all government databases.[27] Maisha Namba cards have been issued in Kenya since 2023,[28] phasing out the old ID cards which are still considered valid for those who held them until they either lose them or willingly apply for a replacement Maisha Namba card.

2.2.2 Huduma Kenya Service Delivery Programme

Huduma Kenya Service Delivery Programme, established in 2014 to ensure access to effective, efficient and citizen-centric public services through one-stop shops, is operationalised through four key service delivery channels: a network of 59 Huduma Centres spread throughout all 47 counties, a Huduma Contact and Tele-Counselling Centre which can be reached by dialling 1919, Huduma Mashinani which involves outreach initiatives, and digital and mobile platforms accessible via the website www.hudumakenya.go.ke and the USSD code *1919#.[29] These channels allow self-service, assisted and digital government services across various government ministries.[30]

Huduma Kenya platforms play a crucial role in enhancing access to government services in Kenya, serving as integrated service delivery points that bring various governmental departments and services under one roof. This innovative approach simplifies the public's interaction with the government, making it more accessible, efficient, and user-friendly.[31]

Huduma Kenya platforms are a one-stop-shop for numerous government services, including the issuance of national IDs, passports, and birth certificates, among others.[32] By centralising these services, the channels reduce the time and travel previously required for citizens to access multiple government offices. This setup not only saves time but also reduces the overall cost of accessing these services, improving the efficiency and convenience for the public.

Huduma Kenya platforms are at the forefront of digitising government services, offering electronic platforms alongside traditional counter services.[33] This dual approach caters to all citizens, including those who are tech-savvy and those who prefer or require face-to-face interactions. By promoting digital services, the platforms facilitate quicker service delivery and reduce physical queues.

Beyond simply processing transactions, Huduma Centres engage in significant community outreach to educate the public on available services and how to access them.[34] These centres often conduct local campaigns and workshops, particularly in rural and underserved areas, to ensure that all citizens, regardless of their location or socio-economic status, can benefit from government services.[35] This proactive approach helps bridge the gap between the government and the communities it serves.

Huduma Kenya platforms also play a key role in collecting feedback from citizens on the quality of government services.[36] This feedback is crucial for continuous improvement and helps the government address any inefficiencies or corruption in service delivery.[37] The platforms are equipped with mechanisms for feedback collection, and they actively encourage users to rate their service expe-

27 ibid, 24

28 Directorate of Immigration Services, 'Issuance of Maisha Card IDs' <https://immigration.go.ke/issuance-of-maisha-card-ids/> accessed 29 April 2024.

29 Huduma Kenya, 'About Us' <https://www.hudumakenya.go.ke/aboutus> accessed on 29 April 2024.

30 ibid.

31 Abdu M et al 'Making Devolution Work for Service Delivery in Kenya' International Development in focus. February 2022 <https://openknowledge.worldbank.org/server/api/core/bitstreams/16d95d32-c4b6-578e-b5b9-e0f4a732bf1b/content> accessed on 30 May 2024.

32 Huduma Kenya (n 104)

33 Abdu M et al 'Making Devolution Work for Service Delivery in Kenya' International Development in focus. February 2022

34 <https://publicadministration.un.org/unpsa/Portals/0/UNPSA_Submitted_Docs/2018/FC492A28-322F-4A3B-8A28-9A86C7B83213/HUDUMA%20MASHINANI-%20PRESENTATION.pdf?ver=2018-02-09-045353-627> accessed on 30 May 2024

35 ibid.

36 Abdu M et al, 'Making Devolution Work for Service Delivery in Kenya' International Development in focus, February 2022

37 ibid.

rience, fostering a culture of transparency and accountability within public service provision.

2.2.3 eCitizen

eCitizen is the main e-government platform in Kenya.[38] The online platform, which launched in 2014, provides access to over 24,000 government services making it a one-stop digital hub for citizens.[39] The integration of mobile money services ensures streamlined payments and accountability. Daily transactions on the platform grew to KES 100.8 billion in FY 2023-2024 compared to KES 26.4 billion in FY 2022-2023, reflecting better efficiency and expanded services.[40] The state plays a critical role in the management of eCitizen through the Ministry of ICT and the Digital Economy together with the ICT Authority. Local firms like Pesaflow Limited, WebMasters Kenya and Olive Tree Media Limited handle payments, technical maintenance and operational support while infrastructure is provided by foreign cloud providers such as Microsoft and Amazon Web Services (AWS).[41]

2.2.4 Gava Mkononi

Gava Mkononi (Swahili for government in your palm) allows citizens, through either a mobile app or the USSD code *2222#, to access services via eCitizen and Huduma Centres. It is state owned and managed by the ICT Authority. However, foreign companies are involved in technical infrastructure and cloud hosting.[42]

Other key e-government services and platforms in Kenya include iTax, managed by KRA that enables tax compliance online;[43] e-Justice System, managed by the Judiciary that facilitates court processes and procedures online;[44] and the Integrated Financial Management Information System (IFMIS) that digitalises financial budgeting, control and planning by the government.[45] All these digital services contribute to the growth of e-governance in Kenya.

2.3 Contextual Analysis of Digital Government Services and Digital ID in Zambia

2.3.1 Digital ID in Zambia

The Zambian government declared its intention to transition to biometric based digital identity in 2008. By March 2022, the details of about 15,000 Zambians had been captured to implement the National Registration Information System (INRIS) biometric digital identity system. The government cited increased security of the identity system as the main reason for implementing this system, to ensure that non-Zambian individuals do not arbitrarily register under the old paper-based identity cards.[46] By November 2023, over one million Zambians had enrolled, with expectations of enrolling 10 million people in the coming decade in a country of about 20 million.

The digital identity system is being established partly under the 2014-2019 National Strategic Action Plan for Reforming and Improving Civil Registration and Vital Statistics.[47] This Action Plan enabled the widespread registration of newborn babies and the provision of birth certificates to ensure that all individuals were registered from birth.[48] Zambian citizens must register for a National Registration Card (NRC) once they turn 16. In 2017, the government introduced an electronic NRC (eNRC) which is now transitioning to the biometric digital ID under the

38 E-Citizen 'Government of Kenya services simplified: All your government records unified' <https://accounts.ecitizen.go.ke/en> accessed 09 May 2025.

39 James Ayugi, 'Why eCitizen is a Game-Changer for Kenyans: Benefits and Impact' (LinkedIn, 2024) https://www.linkedin.com/pulse/why-ecitizen-game-changer-kenyans-benefits-impact-james-ayugi-ayu4f accessed 05 May 2025.

40 Mbadi, 'Mbadi says e-Citizen tripled its revenue to Sh100 billion in one year' (Eastleigh Voice, 18 September 2024) https://eastleighvoice.co.ke/business/79439/mbadi-says-e-citizen-tripled-its-revenue-to-sh100-billion-in-one-year accessed 09 May 2025.

41 ibid.

42 Techcabal, 'Kenya's e-gov app Gava Mkononi will integrate over 5,000 services' <https://techcabal.com/2023/07/05/kenyas-ecitizen-platform-integrated-into-gava-mkononi/> 9 June 2025.

43 Kenya Revenue Authority, 'iTax-KRA' <https://itax.kra.go.ke/KRA-Portal/> 9 June 2025.

44 Kenya Judiciary, 'E-filling is the solution to efficient Judiciary' <https://judiciary.go.ke/e-filling-is-the-solution-to-efficient-judiciary/> 9 June 2025.

45 Finance Kenya, 'Integrated Financial Management Information System' 'https://www.finance.gov.mw/index.php/departments/accountant-general/ifmis> 9 June 2025.

46 Ayang Macdonald, 'Biometrics Registration for Zambia's New National ID System Underway | Biometric Update' (www.biometricupdate.com 14 March 2022) <https://www.biometricupdate.com/202203/biometrics-registration-for-zambias-new-national-id-system-underway > accessed 4 December 2023.

47 Calum Handforth and Matthew Wilson, 'Digital Identity Country Profile: Zambia' (2019) <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Zambia.pdf > accessed 11 June 2024.

48 ibid.

Integrated National Registration Information System (INRIS).[49] The system uses the Modular Open Source Identity Platform (MOSIP) to ensure interoperability with key government services such as financial institutions via KYC processes and healthcare records.[50] MOSIP is developed and maintained by the International Institute of Information Technology Bangalore (IIIT-B).[51] It provides an open-source platform for development of a secure digital identity system supporting biometric enrolment and authentication.[52] It has allowed Zambia to implement a digital ID system that promotes digital inclusivity.

In June 2024, Zambia joined the 50-in-5 coalition of countries.[53]

2.3.2 Smart Village

The smart village project in Zambia aims at bridging the urban-rural digital divide making e-government services more accessible.[54] This is done through connecting local communities to electricity and internet and delivering essential services.[55] The project is in line with the National Electronic Government Plan (NEGP) 2023–2026 whose focus is efficient e-government.[56] The government owns all the infrastructure like communication towers, solar grids and digital equipment.[57] The project is managed in partnership with the Zambian Ministry of Technology and Science and Huawei, which acts as the technology provider for digital classrooms.[58] Zambia and Huawei signed a memorandum of understanding to establish 100 smart villages across Zambia with the aim of providing internet and electricity access,[59] with Huawei supplying digital classroom technologies such as IdeaHub interactive platforms and electronic blackboards to enhance digital literacy in rural areas.[60]

Other external partners include ENGIE which supports rural electrification by deploying mini grid solutions.[61] Under the Increased Access to Electricity and Renewable Energy Production (IAEREP) programme, ENGIE has launched five solar mini grids of 5.7MW capacity in total.[62] The mini grids supply electricity to educational institutions, government offices and households. Through its subsidiary Mysol Grid Zambia, ENGIE oversees the construction, operation, ownership and maintenance, helping expand digital infrastructure in Zambia.[63]

2.3.3 Digital Zambia Acceleration Project (DZAP)

DZAP is a national initiative whose focus is on accelerating Zambia's digital transformation and advancing e-government. It focuses on expanding digital infrastructure and internet in rural areas, digitising key government infrastructure through platforms like the Zamportal, and securing digital infrastructure like digital ID and e-signature. DZAP has enabled safe, seamless access to e-government platforms and digital transactions.[64]

Digital ID and Trust services are a core component of DZAP that aim to modernise public service delivery through secure identity verification. It plays a critical role in citizen identification through a biometric-based digital ID system for public and

49 ibid.

50 Zambia gets $100M World Bank grant and MOSIP boost for digital identity upgrade, Biometric Update (4 August 2024) https://www.biometricupdate.com/202408/zambia-gets-100m-world-bank-grant-and-mosip-boost-for-digital-identity-upgrade accessed 2 July 2025.

51 MOSIP, 'Modular Open-Source Identity Platform - GitHub' https://github.com/mosip accessed 2 July 2025.

52 ibid.

53 50-in5, 'Zambia Joins 50-in-5' <https://50in5.net/zambia-joins-50-in-5/> accessed 10 July 2025.

54 HUAWEI, 'Ministry of Technology and Science of Zambia and Huawei Jointly Launch the Global Smart Village Showcase, Exploring New Digital Transformation Modes for Villages' <https://www.huawei.com/en/news/2025/3/mwc-smart-village-showcase> accessed 08 May 2025.

55 ibid.

56 Smart Zambia Institute, ***National e-Government Plan 2023*** (Republic of Zambia 2023) https://www.szi.gov.zm/wp-content/uploads/2023/08/Final-National_e-Government_Plan_-2023-Final-17.08.2023.pdf accessed 08 May 2025.

57 ibid.

58 ibid.

59 Huawei, 'Huawei, Government of Zambia, to Transform 100 Villages in Zambia, Make them Smart Communities' (Huawei, 17 July 2024) https://www.huawei.com/en/news/2024/7/smart-village-inclusive-connectivity accessed 2 July 2025.

60 ibid.

61 MySol Grid Zambia (ENGIE) to construct 60 mini-grids – USD 7.5 million debt transaction signed with Cygnum Capital Asset Management (Rural Electrification Agency, 30 June 2023) https://www.ruralelec.org/mysol-grid-zambia-engie-construct-60-mini-grids-usd-75-million-debt-transaction-signed/ accessed 2 July 2025.

62 ibid.

63 ibid.

64 The World Bank, 'Appraisal Environmental and Social Review Summary Appraisal Stage' <https://documents1.worldbank.org/curated/en/099010325090041313/pdf/P5050941c5aafd06919ffa1b9afc365c1de.pdf> accessed 08 May 2025.

private services.[65] Trust services include e-signature which enhances transparency and reduces fraud. The project has led to the digitisation of 7.1 million legacy ID records. Through biometric enrolment, data for over 1.3 million citizens has been collected.[66] The initiative is supported by foreign institutions like the World Bank which offers funding, through a $100 million commitment, and technical expertise.[67] The World Bank also provides project management support and capacity-building.[68]

2.3.4 Digital Public Service Transformation

In 2024, Zambia embarked on digital public service transformation aiming to become a digital economy and revolutionise public service delivery. This process is spearheaded by the Ministry of Technology and Science while SMART Zambia Institute owns the project.[69] The state sets strategy and oversees implementation while foreign partners like the World Bank and UNDP provide funding, technical support, and capacity-building.[70] South Africa's Mint Group, also supported Zambia's new digital public service platform.[71]

Other partners and providers include Mosip for e-Signet and eKYC to streamline electronic identity verification and digital signatures, OPENG2P to manage social benefits to ensure efficient and accurate distribution, and MOJALOOP for person-to-government (P2G) and government-to-person (G2P) payments to facilitate seamless financial transactions.[72] However, these partnerships pose vendor lock-in risks arising from the dependency on external partners as well as data sovereignty concerns, demonstrating the need for privacy mechanisms to protect sensitive citizen data.[73]

2.4 Concerns and Challenges Facing Rollout of Digital Identity and Government Digital Services in Kenya and Zambia

The rollout of digital identity and government digital services in Kenya and Zambia faces a myriad of concerns and challenges that impact their effectiveness and adoption. These challenges are examined below.

2.4.1 Legislative Challenges

There are legislative issues arising from the implementation of digital identity stemming from an inadequate legislative regime to govern digital identity. The existing legislative frameworks are poorly drafted and implemented since privacy issues and risks to other human rights violations are not addressed.[74] For instance, the issue of digitised marginalisation emerged in the research process, highlighting warnings about lingering colonial identification systems. Digitising these discriminatory identity systems without addressing the existing issues only perpetuates them, leaving marginalised groups behind. This is particularly the case when digital identity implementation is made mandatory and where government services can only be offered on the condition of having a digital ID.

In Kenya, the Nubians, migrants, refugees, people living in remote areas and other marginalised groups face digitised discrimination arising from the existing discrimination in local identity regimes. During the rollout of Huduma Namba, the mandatory requirements were: a valid Kenya passport or a Kenya national ID card for persons aged 18 years and above and a certificate of birth for persons below 18 years.[75] However, these marginalised groups have historically struggled to obtain these documents, raising fears of digitised discrimination as

73 World Bank, 'Digital Public Infrastructure and Development: A World Bank Group Approach' (Digital Transformation White Paper, Volume 1, 2024) https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf accessed 2 July 2025.

74 Anri Van Der Spuy and others, 'Comparative Analysis of Findings from Ten Country Case Studies towards the Evaluation of Socio-Digital ID Ecosystems in Africa' (2021) <https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf > accessed 16 November 2023.

75 Republic of Kenya, 'Huduma Namba Registration' <https://www.kenyaembassyaddis.org/2019/05/huduma-namba-registration/> accessed 10 July 2025.

they would be unable to transition to digital IDs like other Kenyans. Children born from relationships between refugees and Kenyan citizens were also at risk of being excluded as a result of not being recognised by article 14 (1) that guarantees that anyone is a citizen if by the time of their birth either of their parents was a Kenyan, with the Petition E011 of 2022 by Haki na Sheria ruling by Justice John Onyiego directing a change of the citizenship law as a remedy.[76]

In Kenya, the existing legislation related to digital ID and data protection includes the Data Protection Act (2019).[77] This Act provides a legal framework for the protection of personal data and regulates the processing of personal data in Kenya. Despite having this legislative framework in place, the country faces several challenges in its regulatory frameworks related to digital ID.

One of the primary challenges is the lack of comprehensive implementation of data protection regulations.[78] While laws exist, gaps in enforcement and compliance mechanisms hinder the full realisation of data protection and privacy rights. Limited oversight and enforcement further compound the issue, with regulatory bodies facing challenges in monitoring and ensuring compliance with data protection laws. Insufficient resources, capacity, and expertise within these bodies impede their ability to effectively regulate digital ID systems.[79]

Moreover, ensuring interoperability between different digital ID systems and managing data sharing between government agencies and private entities present challenges in terms of data security, privacy protection, and consent management.[80] Additionally, a lack of public awareness and education regarding data protection rights, digital ID systems, and the implications of sharing personal data contribute to challenges in the regulatory frameworks. This lack of awareness can lead to misconceptions, mistrust, and misuse of digital ID systems.

In Zambia, several legislative challenges exist in the realm of digital ID systems and data protection that need to be effectively addressed to ensure compliance and successful implementation. Enforcement and compliance issues pose significant hurdles in Zambia's data protection landscape. While laws may be in place such as the Data Protection Act of 2021, the effectiveness of enforcement mechanisms and monitoring compliance with data protection regulations remain critical.[81] Inadequate enforcement can lead to data breaches, misuse of personal information, and a lack of consequences for non-compliant entities.[82] Strengthening regulatory oversight and building the capacity of regulatory bodies, such as the Zambia Information and Communications Technology Authority (ZICTA), are essential steps to ensure effective monitoring and enforcement of data protection laws.

Additionally, the harmonisation of laws and regulations with international standards presents a challenge for Zambia. Aligning the country's legislative framework with global data protection norms is crucial for enhancing interoperability, facilitating cross-border data flows, and strengthening data security measures.[83] Furthermore, addressing public awareness and education gaps on data protection rights and digital privacy issues is vital to empower

76 The Standard, 'Children born of Kenyans with refugees win citizenship case' <https://www.standardmedia.co.ke/national/article/2001524595/children-born-of-kenyans-with-refugees-win-citizenship-case> accessed 10 July 2025.

77 Data Protection Act No. 24 of 2019.

78 Melody Musoni, Ennatu Domingo and Elvis Ogah, 'Digital ID systems in Africa: Challenges, risks and opportunities,' 2023 https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-in-Africa-EC-DPM-Discussion-Paper-360-2023.pdf accessed 15 May 2024.

79 O Otele. 'KENYA'S DATA PROTECTION REGIME: CHALLENGES AND FUTURE PROSPECTS.' Journal of African Politics (2021). https://doi.org/10.58548/2021jap101.6688 accessed 15 May 2024.

80 Joseph Owuondo. 'Establishment and Nationalization of Innovative Repository in Kenya: A Collaborative Approach to Scholarly Data Management.' International Journal of Research and Innovation in Social Science (2023). https://doi.org/10.47772/ijriss.2023.71017 accessed 16 May 2024.

81 S Phiri. 'Zambia Digital Rights Landscape Report.' (2021). https://doi.org/10.19088/IDS.2021.007 accessed 16 May 2024.

82 Aaron Zimba, George M. Mukupa and Victoria Chama. 'Emerging Mobile Phone-based Social Engineering Cyberattacks in the Zambian ICT Sector.' ArXiv, abs/2212.13721 (2022). https://doi.org/10.48550/arXiv.2212.13721 accessed 20 May 2024.

83 Mohamed Aly Bouke, Sameer Hamoud Alshatebi, Azizol Abdullah, Korhan Cengiz and Hayate El Atigh. "African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions." ArXiv, abs/2307.01966 (2023). https://doi.org/10.48550/arXiv.2307.01966 accessed 20 May 2024.

individuals to protect their personal data and advocate for their privacy rights effectively.

2.4.2 Gender and Systemic Inequalities

The proposed and deployed digital national services, including digital biometric ID in Africa, reflect a complex interplay of socioeconomic, cultural, and political factors. While these technologies can potentially enhance efficiency and inclusivity, their implementation often exacerbates gender disparities. Women in Kenya and Zambia, especially those in rural or marginalised communities, face challenges accessing and utilising digital services due to limited technological literacy, financial constraints, and cultural barriers.[84] Therefore, a comprehensive analysis of the power dynamics embedded in these digital initiatives is crucial to ensure that they empower rather than marginalise women, fostering an inclusive and equitable digital landscape across the continent.

In analysing the implications of mobile phone ownership disparities for the accessibility of digital ID systems, it becomes evident that gender inequality significantly impacts the effective implementation of digital identification, particularly in Kenya.[85] Goal five of the Sustainable Development Goals (SDGs) emphasise the importance of using technology to empower women. However, the data presented by the Kenya National Bureau of Statistics (KNBS) in collaboration with UN Women shows a nuanced landscape where women are systematically disadvantaged in terms of mobile phone ownership, a precursor to accessing digital ID systems.[86]

Statistics by KNBS in 2022 showed that female mobile phone ownership stood at 47.0%, slightly lower than male ownership at 47.6%. In terms of mobile phone usage, 55.2% of females used mobile phones compared to 55.1% of males, showing a minimal gender difference in usage despite ownership rates.[87] In rural areas, the gap in mobile phone ownership is slightly more pronounced, with 40.3% of females owning mobile phones compared to 40.7% of males. Usage rates in rural areas show females at 48.2% and males at 47.9%, indicating that even with slightly lower ownership, females in rural areas are using mobile phones at a slightly higher rate than males.[88] Urban areas display a clearer disparity in both ownership and usage. Female mobile phone ownership in urban settings is at 62.0% compared to 63.2% for males. Usage rates are 70.7% for females and 71.4% for males. This suggests that while more females in urban areas own and use mobile phones compared to their rural counterparts, they still lag slightly behind males in these metrics.[89]

These disparities in mobile phone ownership and usage between genders can impact access to digital IDs. Since mobile phones are a key platform for digital identification processes, lower ownership and usage rates among females could hinder their ability to access digital services and IDs. This is particularly crucial in rural areas where technology access barriers are already higher.

In Zambia, addressing systemic inequalities is paramount for achieving inclusive digital identity ecosystems. Gender diversity within financial institutions and a gender-lens approach in financial product differentiation is advocated to bridge the gap between men and women.[90] Pervasive gender gaps in various spheres of national development are highlighted, attributing them to entrenched discrimination and traditional practices.[91] It under-

84 ibid.

85 President Ruto unveils government services <PRESIDENT RUTO UNVEILS ONLINE GOVERNMENT SERVICES – The Official Website of the President of the Republic of Kenya> accessed 24 May 2024.

86 Kenya National Bureau of Statistics, 'Preliminary Report on Sustainable Development Goals,' <KNBS-Preliminary-Report-on-Sustainable-Development-Goals.pd> accessed 24 May 2024.

87 Kenya National Bureau of Statistics, 'Women and Men in Kenya Facts and Figures 2022' *(KNBS, 2022)*<Women and Men in Kenya Facts and Figures 2022 - Kenya National Bureau of Statistics (knbs.or.ke)> accessed on 14 June 2024.

88 ibid.

89 ibid.

90 ibid.

91 Sharon Nsana and Harrison Daka. "Strengthening Gender Equality in Decision Making in Public Administration in Zambia." International Journal of Research and Innovation in Social Science (2023). https://doi.org/10.47772/ijriss.2023.7011028 accessed 4 June 2024.

scores the potential of digital identity services, particularly mobile network operators, to address systemic inequalities and empower women and girls.[92]

The transition towards electronic National Registration Cards (eNRC) in Zambia signifies a critical step towards modernising its identity infrastructure. Digitising enrolment processes and databases is crucial for fortifying functional identity registers. However, gender disparities in NRC access and usage persist due to societal norms, necessitating targeted interventions to ensure equitable access for all citizens.[93]

2.4.3 Exclusion of Individuals and Communities

Inclusivity and access to digital identity systems present another set of challenges, particularly concerning marginalised populations.[94] Kenya's Nubian community has for decades faced systemic exclusion and discrimination, hindering their access to essential identification documents.[95] Despite multiple generations of Nubians living in the country, they continue to face barriers in acquiring national IDs which are prerequisites for enrolling in the digital ID system.[96] This exclusion exacerbates their marginalisation and denies them access to crucial services and opportunities.

The process of obtaining an ID in Kenya is governed by the Registration of Persons Act,[97] which grants registration officials considerable discretion. For Nubians, this process involves a rigorous vetting procedure that requires them to prove their lineage and nationality through local leaders, community elders, and various officials.[98] This multi-layered vetting process is unique to Nubians and a few other marginalised communities, creating significant barriers to obtaining IDs.

Moreover, the vetting committees, established in the 1980s, were initially intended to prevent non-Kenyans from border regions from acquiring Kenyan citizenship.[99] However, Nubians, despite residing predominantly in non-border areas like Kibra in Nairobi, are subjected to this process. The lack of statutory guidelines for these committees results in inconsistent and often discriminatory practices.

The exclusion from digital ID systems has profound implications for the Nubian community. Without IDs, Nubians are denied access to essential public services, educational opportunities, formal employment, and political participation.[100] They also face harassment and suspicion from authorities, further marginalising them within Kenyan society.

The persistent delays in issuing IDs to Nubians, often taking significantly longer than for other communities, highlight the systemic nature of their exclusion. Reports indicate that Nubians experience an average wait time of at least eighteen weeks to receive their IDs, compared to shorter periods for other groups.

92 G. Stam. 'Access to Digital Platforms: Can 'Mobile' Network Coverage Reports be Relied Upon? Observations from Rural Zambia and Zimbabwe.' ArXiv, abs/2108.10086 (2021).

93 Accelerating Digital Transformation in Zambia, https://openknowledge.worldbank.org/server/api/core/bitstreams/cb9e3d5a-fd0e-58b6-95c8-34520b7cbf30/content accessed 23 February 2024.

94 Rose Mosero. 'Analysing the impact of Digital ID frameworks on Marginalised Groups in Sub-Saharan Africa.' Social Science Research Network (2021). https://doi.org/10.2139/SSRN.3797506 accessed 22 April 2024.

95 Natalie Kiilu, 'Indirect Discrimination: Huduma Namba (Digital Identification) and the Plight of the Nubian Community in Kenya' (2022) 7 Strathmore L Rev 17 accessed 23 May 2024.

96 ibid, 20.

97 Registration of Persons Act, Chapter 107 Laws of Kenya.

98 'Kenyan's Nubian Minority Pushes Forward for Equal Treatment'(*Relief Web*, 15 May 2017) <Kenya's Nubian Minority Pushes Forward for Equal Treatment - Kenya | ReliefWeb> accessed on 14 June 2024.

99 Lucianna Thuo, 'Ending the Oppression Olympics: Promoting the Concomitant Political Participation of Marginalised Groups in Kenya' (2021) 5 Strathmore Law Journal 49

100 Cherotich Kinei, 'In pursuit of belonging: The Nubian Struggle' (*Fair planet,* 25 April 2015) <In pursuit of belonging: the Nubian struggle | FairPlanet> accessed on 24 May 2024.

2.4.4 Data Governance and Privacy Protection

Security and data protection emerge as critical challenges in the implementation of digital identity systems.[101] Cybersecurity threats and data privacy concerns pose significant risks that need to be addressed to build trust and confidence in these systems. Governments must prioritise addressing security factors such as identity theft, surveillance, discrimination, and inequality to mitigate potential risks and safeguard user data and privacy.

In both Kenya and Zambia, there are concerns over biometric data overcollection without a clear basis or regulatory safeguards. There are also concerns over lack of security and transparency in government data-sharing practices. There is also a general disregard for existing data protection laws.

Kenya has in the past grappled with data protection in the roll out of identity documents, notably with the rollout of Huduma Namba. In the case of *R v Joe Mucheru and Others*,[102] the applicants alleged that the rollout of Huduma cards violated the DPA, specifically the requirement for a data protection impact assessment (DPIA). They requested the court for an order of certiorari to quash the decision to roll out Huduma cards for being ultra vires, and order of mandamus to compel the respondents to conduct a DPIA as required by section 31 of the DPA. In its determination, the court granted the order of mandamus and certiorari, mandating that the government conduct a DPIA before implementing Huduma Namba.[103]

In addition, digital government service platforms often rely on data-driven decision-making, which can further perpetuate biases if the data used in these systems reflect historical inequalities.[104] Machine Learning is a significant contributor to gendered biases in the establishment of digital ID regimes when systems are trained using biased data.[105] Additionally, the deployment of digital biometric ID requirements may raise concerns related to privacy and security, disproportionately affecting women who may already be vulnerable to discrimination.

101 Ayei E. Ibor, Mark Hooper, Carsten Maple and G. Epiphaniou. 'Trustworthy Cross-Border Interoperable Identity System for Developing Countries.' ArXiv, abs/2310.16562 (2023). https://doi.org/10.48550/arXiv.2310.16562.

102 R v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology and others ***ex parte*** Katiba Institute and Yash Pal Ghai [2022] eKLR accessed 14 May 2024.

103 Musoni M, Domingo E and Ogah E, 'Digital ID systems in Africa: Challenges, risks and opportunities', 2023, 23<Digital ID systems in Africa: Challenges, risks and opportunities – ECDPM> accessed 14 May 2024.

104 Lilian Orero, 'The Gender Equality Mirage: From Human Bias to AI Bias in Digital ID Systems in Africa' (2023) https://cipit.org/the-gender-equality-mirage-from-human-bias-to-ai-bias-in-digital-id-systems-in-africa/ accessed 4 June 2024.

105 Md. Arshad Ahmed, Madhur Chatterjee, Pankaj Dadure and Partha Pakray. "The Role of Biased Data in Computerized Gender Discrimination." 2022 IEEE/ACM 3rd International Workshop on Gender Equality, Diversity and Inclusion in Software Engineering (GEICSE) (2022): 6-11. https://doi.org/10.1145/3524501.3527599 accessed 15 May 2024.

Image Source: vecteezy.com

PART THREE

FINDINGS FROM SURVEYS DONE IN KENYA AND ZAMBIA

3.1 Introduction

To understand institutional and organisational challenges in the governance of digital services data and biometric ID data in Kenya and Zambia, CIPIT surveyed participants from the government, civil society organisations (CSOs) and the private sector, gathering and analysing responses from 10 CSOs, 10 government and five private sector organisations in Kenya and 10 CSOs in Zambia. Government and private sector participants in Zambia were reluctant to respond because of the political climate in the country.

3.2 Finding From the Surveys Done in Kenya

3.2.1 Responses from Civil Society Organisations

The surveyed CSOs include Refugee International, Access Now, Digital Rights and Freedoms Regional Hub, Haki na Sheria Initiative, KICTANet, Nubian Rights Forum, Amnesty International Kenya, Advanced ID & Electronics, Centre for Minority Rights Development (CEMIRIDE), Haki Centre, and Namati Kenya. These CSOs engage with a wide array of government platforms spanning eCitizen, travel documents, digital ID systems like Maisha Namba, NHIF (now SHIF), KRA's iTax portal, and the Judiciary's e-filing system. Their collective experiences paint a vivid picture of Kenya's evolving digital landscape, revealing both the promise and the persistent challenges of achieving inclusive digital governance.

3.2.1.1 Barriers to Digital Access for Marginalised Communities

Of significant concern is the persistent exclusion of marginalised groups from accessing government digital services. These groups include refugee populations, ethnic minorities and indigenous communities, as well as majority-Muslim communities in Northern Kenya and the Coast, all of whom struggle to obtain the official identification documents needed to use the government's digital service platforms. Digital illiteracy and infrastructural limitations further exacerbate these challenges.

3.2.1.2 Biometric ID and Digital Identity Implementation

Many CSOs report that biometric data is required for accessing key services, including national identification, SHIF, and voter registration. However, concerns persist regarding the risk of exclusion due to technical errors, lack of clear regulations, and gaps in oversight mechanisms. The centralisation of biometric data without adequate transparency is also a major issue, particularly in relation to systems such as Maisha Namba.

CSOs advocate for biometric ID systems to comply with human rights and data protection standards, with legal challenges against aspects of biometric registration continuing to be a significant area of focus.

3.2.1.3 Regulatory Frameworks Governing Digital Services and Biometric Data

Many CSOs note that the governance of digital services and biometric ID data in Kenya is primarily shaped by the Constitution of Kenya (2010), the Data Protection Act (2019), the Access to Information Act (2016), the Registration of Persons Act (CAP 107), the Births and Deaths Registration Act (CAP 149), the Kenya Information and Communications Act (KICA)(2022), the Computer Misuse and Cybercrimes Act (2018), and the Digital Health Act (2023) among others.

Despite the existence of these frameworks, CSOs have raised concerns about weak enforcement and regulatory gaps that undermine their effectiveness, such as the inconsistent implementation of the Data Protection Act, and questions over the funding challenges, independence and enforcement capacity of the Office of the Data Protection Commissioner

(ODPC). Furthermore, key documents such as Data Protection Impact Assessments (DPIAs) are rarely made public, leading to opaque decision-making processes that further erode public trust.

Another recurring concern is the limited public participation in digital governance policymaking. Many CSOs report that regulatory decisions around digital services and biometric ID systems are often made without meaningful engagement with affected communities. As a result, policies and systems may inadvertently reinforce exclusion, particularly for marginalised groups. To address these challenges, CSOs emphasise the need for greater institutional accountability, enhanced oversight mechanisms, and stronger community involvement in regulatory processes.

3.2.1.4 Advocacy and Litigation for Digital Inclusion

CSOs have actively employed advocacy and litigation to challenge exclusionary digital policies and promote inclusive frameworks as shown by their legal action against Maisha Namba and NIIMS (Huduma Namba). Advocacy initiatives have further played a crucial role in shaping policy by drafting memorandums, engaging in public participation processes to advocate for robust data protection laws and inclusive digital ID policies, highlighting digital identity challenges, and advocating for safeguards against exclusion.

3.2.1.5 Capacity Building and Community Engagement

Beyond advocacy and litigation, CSOs invest significantly in digital literacy and capacity-building programmes that facilitate legal identity applications, educate communities on digital identity rights and processes, and share resources with best practices for digital inclusion of PWDs.

Grassroots engagement initiatives empower indigenous groups to navigate digital service platforms, and equip governments with best practices and the most sustainable technology for specific ID projects.

3.2.1.6 Institutional Bodies and Mechanisms for Addressing Data Governance Issues

Various CSOs are actively working to strengthen institutional frameworks to address data governance challenges. In response to concerns about the operational independence and effectiveness of the ODPC, CSOs continue to push for greater transparency in government data handling and the publication of DPIAs to improve accountability.

CSOs have also established internal methods to ensure data security, including regularly reviewing data privacy policies, ongoing internal training on cybersecurity, and robust encryption measures to prevent unauthorised access to sensitive information.

3.2.1.7 Challenges in Data Governance and Privacy Protection

Despite advancements in advocacy and capacity-building, concerns regarding data governance and privacy risks in government digital services remain. Some organisations have raised alarms about the overcollection of biometric data, particularly in the absence of clear justification or regulatory safeguards. Other groups point to the lack of transparency in government data-sharing practices, especially when it comes to cross-agency collaborations. While Kenya's Data Protection Act represents progress, several organisations argue that its enforcement is still insufficient, leaving citizens exposed to potential data breaches and misuse. Moreover, there are ongoing concerns regarding the absence of clear and balanced consent rules.

There is also a growing emphasis on the need for public education on data privacy rights, given that many individuals remain unaware of how their per-

sonal information is collected, stored, and shared. These challenges have led to calls for the establishment of clear accountability mechanisms to protect citizens from data exploitation.

3.2.2 Responses from Private Sector Participants

The private sector plays a crucial role in the implementation and enhancement of government digital services in Kenya. Companies such as Safaricom Plc, Omega Brand, Jalish Trading Company Ltd, Cisco Systems International, and Airtel Kenya have integrated their services with various government digital platforms, facilitating access to national identification systems, online tax filing services, social security programs, and digital healthcare solutions. These organisations provide the necessary technological infrastructure, connectivity, and security frameworks that enable the smooth operation of e-government services.

However, despite their contributions, the private sector faces numerous challenges in ensuring widespread accessibility and security in digital services. Many underserved communities, particularly in remote areas, struggle to benefit fully from these advancements due to digital illiteracy, infrastructure limitations, and stringent identification requirements.

3.2.2.1 Barriers to Digital Access for Marginalised Communities

Despite advancements in digital service delivery, many marginalised communities continue to face significant barriers in accessing government digital services. Private sector organisations have identified key challenges, including limited digital literacy, lack of proper identification, and inadequate infrastructure in remote areas.

In response to limited network coverage and the financial constraints faced by rural populations, refugees, and internally displaced persons (IDPs), the Communications Authority of Kenya partnered with the private sector to provide subsidised internet access through the Universal Service Fund (USF).

Another significant barrier is the lack of proper identification documents, particularly for refugees and stateless people. Private sector partners work with government agencies to facilitate digital ID registration and authentication, and help mitigate challenges that result from the expiration of refugee cards or the inability to get national ID numbers by offering mobile-friendly platforms that simplify access to e-government services.

3.2.2.2 Biometric ID and Digital Identity Implementation

Biometric identification has become a fundamental component of government digital services, with the private sector playing a key role in data collection, storage, and authentication. Many digital services, including financial products offered by telcos, now require fingerprints, facial recognition, retinal scans, and voice recognition to verify identities and enhance security.

However, concerns have emerged regarding data security, exclusion risks, and regulatory gaps in the use of biometric ID systems. Some individuals, particularly PWDs and elderly populations, have experienced challenges in providing biometric data, raising questions about the inclusivity of these systems. Additionally, data-sharing mechanisms between the government and private sector entities remain unclear, leading to concerns about transparency and accountability in biometric data management. To address these issues, private sector players have called for enhanced oversight and the establishment of standardised biometric data policies that ensure compliance with international best practices in data protection and privacy.

3.2.2.3 Regulatory Frameworks Governing Private Sector Participation

The private sector indicated that digital services are regulated by multiple legal frameworks, including the DPA (2019), KICA (2022), the Computer Misuse and Cybercrimes Act (2018), and sector-specific regulations governing digital services. These laws establish guidelines on data security, consumer rights, and the obligations of private entities in managing government-related digital services.

Many private sector organisations have actively contributed to compliance with regulatory frameworks by developing internal policies aligned with national regulations, engaging stakeholders to help them understand regulatory requirements, and advising organisations on compliance solutions.

Despite regulatory frameworks, enforcement inconsistencies and compliance monitoring gaps remain significant concerns. Frequent regulatory changes complicate compliance efforts and lead to implementation uncertainties, and some data handlers fail to adhere to compliance requirements. Addressing these challenges is essential to ensuring a more consistent and effective regulatory environment for digital services.

3.2.2.4 Advocacy and Litigation for Digital Inclusion

Although private companies do not pursue litigation as CSOs do, many have actively advocated for clearer regulatory guidance to advance digital inclusion by promoting a shared understanding of regulations among stakeholders, and providing feedback to policymakers to strengthen regulatory frameworks

Their engagements with regulators through industry consultations and input on policy drafts aim to create an environment where innovative digital services can thrive while ensuring consumer protection and equitable access.

3.2.2.5 Data Governance and Privacy Protection

Ensuring the security and privacy of government-collected data remains a top priority for private sector participants. Many have implemented robust encryption protocols, regular cybersecurity audits, and staff training programmes to strengthen data governance and privacy protection.

To enhance security, some private sector participants have introduced multi-layered measures, including advanced encryption technologies, to safeguard biometric data and prevent unauthorised access. Others have adopted strict internal policies that limit data-sharing with third parties, ensuring compliance with data protection regulations.

However, private sector organisations continue to face challenges such as high compliance costs, evolving cyber threats, and insufficient consumer awareness of data protection rights. In response, they have called for stronger collaboration with regulatory bodies to establish standardised cybersecurity frameworks and promote best practices in data protection.

3.2.2.6 Capacity Building and Public Awareness

In addition to regulatory compliance, some private sector organisations have invested in capacity-building initiatives to enhance digital literacy and data governance awareness through staff training, public awareness campaigns, and stakeholder education.

Despite these efforts, not all organisations are actively involved in capacity-building, with some primarily acting as consumers of biometric data rather than facilitators of digital literacy programs. Addressing this gap requires collaborative efforts among stakeholders to promote a culture of digital

security and informed data usage.

3.2.2.7 Institutional Bodies and Mechanisms for Addressing Data Governance Issues

Private sector players have developed robust internal data governance frameworks to safeguard sensitive information. Many have instituted multi-layered security measures, including regular cybersecurity audits, encryption protocols, and strict access controls. They also rely on internal compliance departments and industry associations that collaborate with regulators. These mechanisms ensure that private sector digital services adhere to the DPA and other relevant regulations.

Private sector participants identified several institutional bodies as responsible for overseeing the implementation of existing regulatory frameworks that govern the provision of government digital services and biometric data in the country. These include the Ministry of Information, Communication, and Technology, the Communication Authority of Kenya and Office of the Registrar of Persons among others. Additionally, national data protection authorities or equivalent government bodies, internal Data Governance and Compliance Departments within organisations, and international standards bodies such as the International Organization for Standardization (ISO) play a crucial role. Other key institutions mentioned include ODPC and regulatory bodies such as the Communications Authority of Kenya, which enforces KICA and SIM card regulations.

3.2.3 Responses from Government Participants

Government agencies play a central role in the provision, regulation, and oversight of digital services in Kenya. Various ministries, commissions, and parastatals have developed e-government platforms to facilitate public service delivery, digital identity management, and taxation. Key agencies involved include the National Transport and Safety Authority (NTSA), Kenya Revenue Authority (KRA), Independent Electoral and Boundaries Commission (IEBC), Directorate of Immigration and Citizen Services, and the National Registration Bureau (NRB).

These institutions operate diverse digital systems that aim to improve efficiency, accessibility, and transparency in public administration.

Despite these efforts, challenges remain, particularly in ensuring digital inclusivity for marginalised communities, securing biometric data, and maintaining compliance with regulatory frameworks. Government agencies acknowledge the need for continuous reforms, investment in secure infrastructure, and enhanced data governance practices to optimise service delivery.

3.2.3.1 Barriers to Digital Access for Marginalised Communities

While government digital services are designed to be accessible to all citizens, some communities face significant barriers in utilising these platforms. Digital literacy, lack of internet access, documentation challenges, and infrastructural limitations hinder access, particularly for individuals in rural areas, refugees, and pastoralist communities.

Government institutions have implemented various initiatives to bridge these gaps, such as establishing Huduma Centres in major towns complemented by mobile registration services. However, accessibility remains a challenge for marginalised communities outside Nairobi.

3.2.3.2 Biometric ID and Digital Identity Implementation

Government agencies rely heavily on biometric identification systems to authenticate users of digital services. Various institutions collect and process biometric data such as fingerprints, facial rec-

ognition scans, and live capture images. All these services heavily rely on the National Registration Bureau database which forms the foundation for their secondary capture and verification of their functional IDs.

However, not all government institutions require biometric data. Some agencies do not collect biometric identifiers, relying instead on alternative authentication methods.

Although biometric systems enhance security and service efficiency, concerns remain about data privacy, security risks, and potential exclusion of disabled individuals who face challenges in biometric enrolment.

3.2.3.3 Regulatory Frameworks Governing Government Digital Services

Sector participants noted that the governance of digital services and biometric ID data in Kenya is guided by several legal frameworks, including the DPA (2019), Access to Information Act (2016), Computer Misuse and Cybercrimes Act (2018), KICA (2022), and the Constitution of Kenya (2010). These laws establish data privacy protections, cybersecurity requirements, and transparency obligations for public institutions.

Government institutions reported a range of challenges in implementing existing data governance frameworks. While the relevant laws and policies provide a solid foundation for protecting personal data and managing digital services, several practical difficulties have emerged during implementation including limited technical infrastructure, low awareness of data protection obligations, human resource constraints, and overlapping or excessively detailed internal policies.

Moreover, financial constraints remain a persistent barrier. Due to limited funding, institutions often struggle to procure and maintain essential data protection technologies. Political challenges, particularly for institutions involved in elections, along with a lack of political goodwill and a trust deficit among political players, may hinder the implementation of some frameworks due to fear of potential setbacks. In addition to these concerns, system fragmentation and a lack of interoperability has undermined biometric identity verification processes.

Finally, security vulnerabilities continue to pose significant risks. Taken together, these challenges highlight the pressing need for clearer regulatory guidance, targeted capacity-building initiatives, sustained political and financial support, and improved coordination among public institutions to fully operationalise existing data governance frameworks.

3.2.3.4 Data Governance and Privacy Protection

Ensuring data security and privacy in government digital services is a top priority, with agencies implementing various security measures such as strict data encryption protocols, user authentication controls, and access restrictions to protect sensitive information.

Despite these measures, government agencies continue to face security challenges, including hacking threats, unauthorised data access, and infrastructure limitations.

To enhance data governance, government institutions have proposed stronger cybersecurity enforcement, capacity-building programmes, and increased investment in secure data storage infrastructure.

3.2.3.5 Capacity Building and Public Awareness

Recognising the need for continuous staff training and public engagement, government agencies have prioritised capacity-building programmes and citizen-centric awareness campaigns to reinforce biometric data security and digital service integrity. These initiatives entail institutional training and nationwide sensitisation to address evolving threats and societal gaps.

Despite progress, challenges persist, including uneven public awareness and rapidly advancing cyber threats. To bridge gaps, agencies advocate for nationwide sensitisation drives and localised training workshops tailored to rural and marginalised populations. Partnerships with third-party service providers also mandate adherence to security standards, ensuring end-to-end protection even in outsourced operations.

By intertwining staff capacity-building with public education, institutions promote a culture of shared responsibility for data security. This dual approach not only strengthens technical defences but also cultivates trust in digital services, ensuring equitable access and compliance across diverse demographics.

3.3 Finding From the Surveys Done in Zambia

3.3.1 Responses from Civil Society Organisations

In Zambia, CSOs have increasingly become central to shaping the country's digital governance landscape. The surveyed organisations include Zambian Cyber Security Initiative Foundation (ZCSIF), Zambian Bloggers Network, Transparency International Zambia, Paradigm Initiative Zambia, Mizhipa Housing Cooperative Society, MISA Zambia, Michenja Sustainable Organisation, Common Cause Zambia, and Advocates for Democratic Governance Foundation. These organisations demonstrate diverse engagements with digital platforms and policy-making processes. Their involvement ranges from interactions with the e-Government Portal (ZAMPORTAL), the Zambia Public Procurement Authority (ZPPA), the Patents and Companies Registration Agency (PACRA), and the ZRA's SmartInvoice and TaxOnline services, to participation in digital ID systems and biometric voter registration.

While their approaches differ, these CSOs collectively contribute to shaping a digital ecosystem that aspires to be inclusive, transparent, and responsive. Their work spans advocacy, digital rights awareness, capacity-building, community engagement, and institutional collaboration, thereby highlighting progress and ongoing challenges in Zambia's digital transformation journey.

3.3.1.1 Barriers to Digital Access for Marginalised Communities

A key theme that emerged from the survey responses was the persistent challenge of digital exclusion, particularly among marginalised groups. Several CSOs reported implementing targeted initiatives to close this gap, like digital literacy programmes, cyber hygiene workshops, e-government support systems, and advocacy on behalf of marginalised communities.

However, this commitment is not universal, with some CSOs targeting some groups and not others.

3.3.1.2 Biometric ID and Digital Identity Implementation

The use of biometric data in accessing government digital services is another area where CSOs have diverse experiences. Most respondents, five out of nine, confirmed that biometric authentication is required for certain services like during enrolment for digital IDs.

Some organisations, however, reported that they

are not required to submit biometric data for access, indicating a lack of consistency in service requirements.

Importantly, concerns were raised regarding the transparency and ethical management of biometric systems, such as a lack of government communication about the purpose of data collection. These issues underscore the need for stronger consent practices and regulatory oversight in biometric identity systems.

3.3.1.3 Regulatory Frameworks Governing Digital Services and Biometric Data

Most organisations demonstrated strong familiarity with existing legal frameworks including the Data Protection Act (2021), the Cyber Security and Cyber Crimes Act (2021), the Electronic Communications and Transactions Act (2021), and the ICT Act (2021). Additional references included the Digital Transformation Strategy (2023 to 2026), the Smart Zambia E-Government Master Plan, and regional frameworks such as the AU Malabo Convention and the SADC Model Law.

Despite this awareness, not all organisations reported equal levels of engagement. Vague or incomplete responses from some suggest a gap in internal technical capacity or familiarity with the legal environment.

This uneven engagement highlights the need to strengthen institutional literacy on digital governance laws among CSOs, particularly those operating at grassroots or community levels.

3.3.1.4 Advocacy and Litigation for Digital Inclusion

In terms of advocacy, many organisations reported meaningful involvement in shaping digital inclusion policies through collaboration with policymakers, public education, and engagement with regulatory agencies. However, formal litigation strategies were notably absent among the surveyed CSOs.

This suggests that most Zambian CSOs favour constructive engagement and policy dialogue over litigation when advancing digital rights and inclusion.

3.3.1.5 Capacity Building and Community Engagement

Capacity-building emerged as a strong focus for several organisations through community-based training, public engagement, and awareness sessions.

However, this momentum is not shared across all actors, with some organisations reporting limited training programmes, a lack of technical capacity, and nascent internal governance frameworks.

As such, there is a pressing need to support institutional capacity development to ensure broader and more effective engagement with digital governance issues.

3.3.1.6 Institutional Bodies and Mechanisms for Addressing Data Governance Issues

On institutional oversight, CSOs cited various regulatory bodies responsible for enforcing digital governance frameworks. These include the Zambia Information and Communications Technology Authority, the Data Protection Commission, and respective line ministries.

Internally, for the private data of the clients they serve, the presence of robust governance mechanisms varied considerably ranging from comprehensive encryption systems and audits to basic practices like password hygiene and regular data backups.

This variation highlights the need for tailored support to help CSOs enhance their internal data governance systems and better align with national regulatory requirements.

3.3.1.7 Challenges in Data Governance and Privacy Protection

Across the surveyed organisations, several persistent challenges continue to undermine efforts to strengthen data governance and privacy protection in Zambia's digital ecosystem. A recurring issue is the limited level of digital literacy and public awareness, particularly within rural communities. In parallel, civil society actors themselves often struggle with inadequate funding and limited technical capacity.

Several organisations also pointed to systemic shortcomings in government transparency and accountability. This lack of clarity has eroded public trust in digital public infrastructure. Furthermore, the absence of an operational Access to Information framework has made it difficult for both citizens and CSOs to scrutinise data handling by public institutions or hold them accountable for lapses.

The problem is further compounded by fragmentation across institutional mandates, with multiple agencies responsible for different aspects of digital services and data governance. This results in poor coordination and limited interoperability of systems, undermining the coherence of the country's digital transformation agenda. In addition, cybersecurity threats and insufficient enforcement of existing laws continue to expose individuals to risks of data misuse, surveillance, or breaches, particularly in relation to biometric information.

Image Source: vecteezy.com

Image Source: vecteezy.com

PART FOUR

ANALYSIS OF SURVEYS DONE IN KENYA AND ZAMBIA

4.1 Introduction

The surveys engaged a diverse range of participants and the scope of inquiry covered various aspects of digital governance, such as the nature of digital services provided, accessibility to marginalised communities, the types of biometric ID data collected, the existence of internal data governance frameworks, mechanisms for protecting sensitive personal data, challenges in ensuring data security, capacity-building needs, regulatory compliance, and approaches to addressing data breaches.

For Kenya, the analysis integrates responses from all three stakeholder groups namely, CSOs, private sector and government agencies. In contrast, the analysis for Zambia is predominantly based on responses from CSOs.

4.2 Analysis of Findings from Kenyan Surveys

The digital landscape in Kenya is shaped by the interplay of government initiatives, private sector innovation, and civil society advocacy. An examination of the survey responses from these three stakeholder groups reveals both progress and persistent challenges in ensuring inclusive and secure digital governance.

4.2.1 Challenges in Digital Access and Inclusion

A significant concern across all surveyed sectors in Kenya is the persistent exclusion of marginalised communities from accessing government digital services. CSOs highlight bureaucratic hurdles faced by refugee populations in registering for digital IDs. They report that ethnic minorities and indigenous communities frequently struggle to obtain official identification. These groups also struggle to access digital services. Beyond documentation, CSOs point to digital illiteracy and infrastructural limitations as exacerbating these challenges, impeding rural communities' ability to interact with online government services.

The private sector corroborates these observations, identifying limited digital literacy, the lack of proper identification, and inadequate infrastructure in remote areas as key barriers. While some entities play a critical role in providing mobile connectivity for many of the government's digital services, many rural populations, refugees, and IDPs still struggle with access due to limited network coverage and financial constraints. Likewise, government agencies acknowledge similar barriers, noting that digital illiteracy, lack of internet access, documentation challenges, and infrastructural limitations hinder access, particularly for individuals in rural areas, refugees, and pastoralist communities.

One notable hurdle to digital access is that birth registration in major towns has been moved to eCitizen which requires an ID card number, refugee card number or alien card number to access, thereby excluding undocumented persons or stateless communities.

The consistent mention across all three stakeholder groups of the lack of foundational identity documents as a primary barrier to digital access reveals a deeply rooted systemic issue. This is not merely a matter of technological access or digital literacy but a question of the very prerequisites for engaging with digital public infrastructure. If foundational identity documents are inaccessible, the entire digital service ecosystem becomes an insurmountable barrier for these populations. This suggests that digital exclusion in Kenya is not solely a technological or educational gap but is profoundly rooted in traditional administrative and legal identity systems.

The digital divide, therefore, exacerbates existing social and economic inequalities, disproportionately affecting already vulnerable populations by denying them access to essential services. Further-

more, while the private sector and government are making efforts to expand connectivity and physical access points, the continued reports of digital illiteracy and infrastructural limitations suggest that these initiatives may not be sufficiently widespread, affordable, or accompanied by the necessary digital literacy programmes to ensure effective utilisation, especially in remote communities. This implies that relying solely on infrastructure rollout is insufficient for achieving true digital inclusion, which requires a holistic strategy integrating infrastructure development with targeted digital literacy programmes, affordability measures, and culturally sensitive outreach.

4.2.2 Biometric ID Implementation and Governance Concerns

Digital identity registration, which holds the keys to all other services, falls under the NRB which has issues of vetting. Vetting has been identified as a barrier to accessing this vital documentation that could allow access to all services on the eCitizen platform. The digital ID is also considered a foundational document for accessing digital government services provided by institutions such as NTSA, KRA and other government departments. NRB has integrated live capture biometrics for issuing identity cards in the country, moving away from ink capture.

The integration of biometric ID systems into government digital services has introduced both opportunities and significant challenges. CSOs report that biometric data, such as fingerprints and facial recognition, is widely required for accessing key services, including national identification, health insurance, and voter registration. However, concerns persist regarding the risk of exclusion due to technical errors, the absence of clear regulations, and gaps in oversight mechanisms. The centralisation of biometric data particularly in systems like Maisha Namba, without adequate transparency, is highlighted as a major issue.

Additionally, private sectors and government agencies rely heavily on biometric identification systems for digital services like financial transactions, voter registration, and identity card issuance, aligning with national digital ID requirements. However, concerns about data security, unclear data-sharing mechanisms, and exclusion risks for vulnerable groups, such as PWDs and the elderly, who struggle with biometric enrolment, have prompted calls for enhanced oversight, standardised policies, and robust data privacy measures to address these challenges.

All three groups acknowledge that biometric systems enhance security and service efficiency. However, CSOs and the private sector explicitly highlight exclusion risks for vulnerable groups, as well as data privacy and security risks. This creates a paradox where a technology designed to secure and streamline access inadvertently creates new barriers and vulnerabilities for specific populations, potentially undermining the goal of universal service access. This suggests that the current implementation of biometric ID systems, while technologically advanced, may be failing on the inclusivity and human rights fronts, necessitating robust DPIAs and the development of alternative verification methods.

Furthermore, the consistent lack of transparency around how sensitive biometric data is collected, stored, and shared, as noted by CSOs (lack of public DPIAs) and the private sector (unclear data-sharing mechanisms), directly undermines public trust. Without clear communication, meaningful public participation, and transparent accountability mechanisms, the widespread adoption of biometric ID systems risks fuelling public distrust, potentially leading to resistance, litigation, and ultimately hindering the effectiveness and legitimacy of national

digital government initiatives.

4.2.3 Data Governance and Privacy Protection Deficits

Despite various measures in place, ensuring data security and privacy in Kenya's digital services remains a persistent challenge. CSOs raise concerns about the overcollection and centralisation of biometric data without clear justification or safeguards, along with opaque data-sharing practices across government agencies. They argue that while the DPA is a step forward, weak enforcement and unclear consent mechanisms expose citizens to misuse and breaches. CSOs also emphasise the need for greater public education, as many individuals lack awareness of how their data is collected, stored, and used. The private sector, meanwhile, has adopted encryption protocols, cybersecurity audits, and staff training but continues to struggle with high compliance costs, evolving threats, and low consumer awareness. These actors call for closer collaboration with regulators to develop standardised frameworks and promote best practices. Government agencies report using encryption, access controls, and authentication systems, with some adhering closely to the law. However, they still face hacking attempts, insider breaches, and infrastructure gaps, as illustrated by the 2023 cyberattack on the eCitizen platform.

The combined concerns from CSOs about overcollection and centralisation of biometric data, and government reports of hacking and insider breaches, underscore a critical vulnerability: while centralising data may improve service delivery, it also creates a single, attractive target for both external and internal threats. This heightens the risk and potential impact of breaches, making robust ethical guidelines, internal controls, and institutional accountability essential. Additionally, the consistent observations by CSOs and the private sector about low public awareness reveal a major knowledge gap between those who manage personal data and the individuals to whom it belongs. This asymmetry disempowers citizens and limits their ability to exercise data rights, highlighting public education as a vital yet often neglected pillar of responsible and effective data governance.

4.2.4 Effectiveness of Regulatory Frameworks

Kenya has a robust legal framework governing digital services and biometric ID data, but key issues arise across civil society, the private sector, and government. Civil society organisations point to weak enforcement, regulatory gaps, limited transparency in government data practices such as the non-disclosure of DPIAs, and insufficient public participation, which contribute to low trust and potential exclusion. The private sector highlights overlapping regulations, frequent legal changes, and inconsistent enforcement, all of which create uncertainty and complicate compliance efforts. Further, government agencies report challenges related to limited technical infrastructure, low awareness of data protection obligations, inadequate staffing, financial constraints, and fragmented systems, which collectively undermine the effective implementation of data governance frameworks.

The consistent pattern across all three sectors suggests that while the legal foundation exists and appears robust in theory, its operationalisation is severely limited by systemic and practical shortcomings. This indicates that the current regulatory environment, though grounded in strong legislation, remains largely ineffective in practice. Addressing this requires a shift from enacting laws to prioritising enforcement capacity, improving inter-agency coordination, and demonstrating genuine political commitment to implementing these frameworks.

4.2.5 Capacity Building and Institutional Weaknesses

Capacity building and institutional strengthening are widely acknowledged as essential for effective digital governance. CSOs lead many of these efforts through initiatives such as training community paralegals, conducting school outreach, and developing resources for the digital inclusion of PWDs. They also promote transparency in government data handling, including advocating for the publication of DPIAs, while maintaining internal safeguards like updated data privacy policies, cybersecurity training, and encryption.

In the private sector, while some organisations engage in staff training and public awareness initiatives, many primarily act as users of biometric data rather than contributors to digital literacy, prompting calls for greater investment in cybersecurity infrastructure and education. Government agencies also prioritise training and awareness campaigns for both staff and the public, aiming to strengthen biometric data security and digital service integrity, though challenges such as low public awareness and fast-evolving cyber threats persist.

The research identified gaps in training, ranging from knowledge of the laws and best practices of data protection and inclusion, that could be solved through regular staff capacity-building. Most of the institutions interviewed did not indicate that they were trained on the new laws on data protection nor were they aware of the need for data protection impact assessments. Government acknowledgments of human resource constraints and limited awareness of data protection obligations, alongside reports of internal misconduct and data breaches, point to human capacity as a key factor in successful digital governance.

These challenges show that technical measures alone are insufficient without continuous investment in human capital; through citizen-focused digital literacy, specialised personnel training, and an ethical institutional culture. The uneven involvement of private sector actors in capacity-building, contrasted with the more consistent efforts by CSOs and some government bodies, reveals a fragmented landscape. This lack of coordination suggests the absence of a comprehensive digital governance blueprint, which risks leaving critical gaps in digital resilience, especially if key stakeholders are not consistently and adequately equipped.

4.3 Analysis of Findings from Zambian Surveys

The assessment of digital governance in Zambia is primarily informed by the perspectives of CSOs because of the absence of data from key state and commercial actors. This limitation must be prominently highlighted as it impacts the comprehensiveness and balance of the overall analysis for Zambia.

4.3.1 Digital Exclusion and Access Barriers

A key theme emerging from Zambian CSOs is the persistent challenge of digital exclusion, particularly among marginalised groups such as refugees, asylum seekers, women and girls, PWDs, and underserved communities. Some organisations have actively rolled out digital literacy programmes, cyber hygiene workshops, and e-government support systems for vulnerable populations. Other organisations have focused on advocating for the inclusion of these marginalised communities in the digital space. Despite these efforts, challenges persist, particularly in peri-urban and rural areas where poor connectivity and limited digital literacy continue to hinder meaningful engagement with digital services. Given the stated data limitations from government and the private sector, the extensive efforts of Zambian CSOs in digital literacy, advocacy for inclusion, and community sensitisation become even more critical. They are effectively filling

a potential void left by other sectors, acting as the primary agents pushing for digital inclusion and digital rights at the grassroots level, often compensating for broader systemic weaknesses. This implies that in contexts where state and private sector transparency or engagement on digital rights might be limited, CSOs emerge as indispensable actors for ensuring digital inclusion and protecting citizen rights, highlighting their crucial role in the national digital transformation agenda.

4.3.2 Biometric ID Transparency and Ethical Concerns

The use of biometric data in accessing government digital services is another area of diverse experiences among Zambian CSOs. Most respondents confirmed that biometric authentication, including fingerprints, facial recognition, and iris scans, are required for certain services. Some organisations, for example, noted that multiple biometric identifiers are collected during enrolment for digital IDs. However, concerns were raised by some CSOs regarding a lack of government communication about the purpose of data collection and concerns about data-sharing practices. The inconsistency in service requirements, with some organisations not being required to submit biometric data, also indicates a lack of uniformity. Like Kenya, Zambian CSOs, even from their external perspective, express concerns about lack of government communication regarding the purpose of data collection and raised concerns about data-sharing practices. This suggests that even without direct government input, CSOs perceive a lack of transparency around biometric data, which is a critical factor in public trust. The inconsistency in service requirements further compounds this, potentially leading to confusion and arbitrary application of biometric mandates. This opacity and inconsistency surrounding biometric data collection and use, even from the limited CSO perspective, indicate a nascent but significant trust deficit. If not addressed through clear communication, standardised practices, and robust oversight, this can lead to public resistance, non-compliance, and a general erosion of confidence in digital ID systems, thereby hindering broader digital transformation efforts and potentially impacting human rights.

4.3.3 Regulatory Awareness and Engagement Gaps

Zambian CSOs generally demonstrated strong familiarity with existing legal frameworks, frequently citing the Data Protection Act (2021), the Cyber Security and Cyber Crimes Act (2021), and the Electronic Communications and Transactions Act (2021). However, not all organisations reported equal levels of engagement. While some CSOs indicated robust interaction with regulators and active promotion of compliance, others provided vague or incomplete responses, suggesting a gap in internal technical capacity or familiarity with the legal environment. This highlights the need to strengthen institutional literacy on digital governance laws among CSOs, particularly those operating at grassroots or community levels. While some CSOs show robust interaction with regulators, others exhibit vague or incomplete responses and a lack of internal technical capacity. This points to a significant disparity in the institutional capacity of CSOs themselves to effectively engage with complex digital governance issues, understand nuanced legal frameworks, and advocate for policy changes. This implies that the effectiveness of civil society as a collective watchdog and advocate for digital rights is undermined by internal capacity gaps. Strengthening the technical and legal literacy of all CSOs, particularly those operating at grassroots levels, is crucial for cultivating a more informed, cohesive, and impactful civil society voice in Zambia's digital

governance debates.

4.3.4 Capacity-Building and Internal Governance Needs

Capacity-building emerged as a strong focus for several Zambian CSOs, with some organisations investing in community-based training on digital safety, ethical data use, and cybersecurity. Other organisations also reported organising public forums and awareness sessions on digital rights. However, this momentum is not shared across all actors, with some CSOs indicating limited or no biometric-specific training programmes, or a general lack of internal technical capacity. Internal governance mechanisms also varied considerably among CSOs, ranging from comprehensive systems with encryption and audits to informal practices like basic password hygiene or policies still under development. The variation in internal data governance practices among CSOs themselves is a critical observation. If CSOs are advocating for strong data governance and privacy from the government and private sector, their own internal practices serve as a critical benchmark for their credibility and effectiveness. A lack of internal rigor can weaken their external advocacy and expose them to the very risks they seek to mitigate for citizens. This implies that to be effective and credible advocates for robust digital governance and data protection, CSOs must first ensure their own internal data governance and capacity-building frameworks are strong and compliant with best practices. This internal alignment reinforces their legitimacy and provides practical experience that can inform their policy recommendations.

4.3.5 Risk Aversion and Governance Decay

The surveys failed to capture perspective from all the government stakeholders in Zambia. The study sought responses from the Ministry of Home Affairs, Department of National Registration, Passport and Citizenship, Ministry of Technology and Science, Smart Zambia Institute (SZI), and Zambia Information and Communications Technology Authority (ZICTA). All these institutions failed to respond to questionnaires despite formal requests made to each of them. This was caused by a tense political climate in the country. It would have been ideal to capture the perspective of government departments to be able to identify the specific needs and challenges in the rollout and implementation of digital government services. This study therefore notes political tension in Zambia as a key challenge impacting government service delivery.

Thus, this study notes the need for training of government officials on how collaboration with CSOs help build public trust especially since Zambia has two ID registers; one for those who have digital IDs and another for those without digital IDs. The culture of fear of collaboration is counterproductive as both are serving the same population and are not competitors.

4.4 Cross-Cutting Key Issues

The analysis of survey findings from Kenya and Zambia reveals several overarching, systemic challenges that transcend national and stakeholder boundaries, significantly impacting the governance of digital services and biometric ID data.

4.4.1 Systemic Digital Exclusion

Across both Kenya and Zambia and consistently reported by all stakeholder groups in Kenya and CSOs in Zambia, the persistent exclusion of marginalised communities from digital services is a critical, multi-faceted issue. It is not merely a technological or educational gap but a deeply entrenched socio-economic and administrative problem. The fundamental requirement for official identification documents (national IDs, birth certificates) often acts as the initial and most significant barrier to digital access, particularly for refugees, stateless persons, and ethnic minorities. This indicates that digital inclusion efforts are frequently hindered by pre-digital administrative hurdles related to civil registration and legal identity. Furthermore, limited network coverage, lack of smartphones, and financial constraints disproportionately affect rural and peri-urban populations in both countries. While some efforts are being made (e.g. Huduma Centres), the persistent digital literacy gap further exacerbates this divide, making meaningful engagement with online services difficult even where infrastructure exists. The inability to register for and access digital services, stemming from a lack of foundational identity documents, perpetuates exclusion from essential services (health, finance, education) and civic participation. Similarly, limited infrastructure, affordability issues, and low digital literacy prevent effective utilisation of available digital services. This situation ultimately reinforces existing social and economic inequalities, potentially creating a two-tiered society where access to essential services and opportunities is contingent on digital presence, thereby leaving behind the most vulnerable segments of the population and hindering equitable national development.

4.4.2 Regulatory Enforcement and Accountability Gaps

Both countries possess legal frameworks designed to govern digital services and data, but their effectiveness is consistently undermined by weak enforcement, regulatory inconsistencies, and a lack of clear accountability, rendering them less impactful than intended. Despite the existence of comprehensive laws (e.g. Data Protection Acts), their practical implementation is hampered by insufficient funding, human resource constraints, and the proliferation of numerous, sometimes overlapping, internal policies that make interpretation difficult. This points to a significant gap between legislative intent and operational reality. Independent oversight bodies, such as the ODPC in Kenya, face challenges related to funding, operational independence, and enforcement capacity. Moreover, regulatory decisions around digital services and biometric ID systems are often made without meaningful engagement with affected communities, leading to policies and systems that may inadvertently reinforce exclusion or fail to address ground realities. The weak enforcement capacity and lack of independence for oversight bodies lead to inconsistent application of laws and limited accountability for data breaches and misuse, which in turn reduces public trust and increases risks to data privacy. The limited public participation in policymaking results in policies that do not adequately address community needs, leading to continued exclusion and suboptimal digital service design.

4.4.3 Transparency and Trust Deficits

A pervasive lack of transparency in data collection, sharing, and overall governance practices, coupled with insufficient public awareness, is systematically eroding trust in digital services and biometric ID systems in both nations. This represents a critical barrier to widespread adoption and legitimacy. Key documents like DPIAs are rarely made public, and there is a consistent lack of clear government communication regarding the purpose of data collection, who controls data, and how it will be stored or shared. This secrecy breeds suspicion and uncertainty among citizens. Many citizens remain unaware of how their personal information is collected, stored, and shared, or of their fundamental data privacy rights. This significant knowledge gap prevents individuals from providing informed consent or effectively seeking redress for potential misuse. In Zambia, the political climate explicitly led to government and private sector participants not sharing information, indicating an environment where transparency might be politically sensitive and directly contributing to a trust deficit. Opaque data practices and insufficient public awareness prevent citizens from providing informed consent or seeking redress, which results in an erosion of public trust in digital services and ID systems. This lack of trust can lead to public resistance to digital services and ID systems, thereby hindering digital transformation and reducing public benefit. Trust is the bedrock of successful digital transformation. Without it, even well-intentioned digital initiatives will face public scepticism and resistance, limiting their reach and effectiveness.

4.4.4 Capacity and Resource Constraints

Across all stakeholder groups and both countries, limitations in technical infrastructure, human resources, and financial investment consistently hinder the effective implementation of digital governance frameworks and the provision of secure, efficient digital services. Limited technical infrastructure, particularly in rural and underserved areas, continues to impede secure data transmission and restrict access to government digital platforms. This creates a fundamental bottleneck for digital service delivery. A persistent shortage of adequately trained personnel, especially around complex areas like biometric data governance, limits the capacity of institutions to effectively apply and monitor existing frameworks. Furthermore, there is an uneven distribution of capacity-building efforts within the private sector and among CSOs, leading to varied levels of expertise across the ecosystem. Institutions often struggle to procure and maintain essential data protection technologies such as encryption systems, secure servers, and backup infrastructure due to limited funding. High compliance costs also pose a significant challenge for private sector participants. Insufficient investment in infrastructure and human resources leads to an inability to implement robust data protection measures and effectively enforce regulations, which results in increased vulnerability to cyber threats, inefficient service delivery, and inconsistent application of policies. These pervasive constraints create a vicious cycle where under-resourced institutions struggle to meet evolving digital demands, leading to persistent vulnerabilities, inefficient service delivery, and a widening gap between policy aspirations and practical realities.

4.4.5 Cybersecurity Vulnerabilities and Data Misuse Risks

Despite efforts to implement security measures, both nations face significant and evolving cybersecurity threats, ranging from external attacks to internal misconduct, posing considerable risks to sensitive digital and biometric data. Incidents like the eCitizen cyberattack in 2023 and reported cases of insider data breaches where officers leaked sensitive information highlight vulnerabilities stemming from both external malicious actors and internal human factors, including attempts by staff to bypass safeguards for personal or financial gain. Concerns about the overcollection of biometric data and its centralisation inherently increase the potential impact and attractiveness of a single breach, making these large datasets high-value targets for cybercriminals. The private sector explicitly notes evolving cyber threats, underscoring the continuous and dynamic nature of the risks, which requires constant adaptation and investment in security measures. System vulnerabilities, human factors (e.g. low awareness, misconduct), and evolving cyber threats lead to an increased risk of data breaches, unauthorised data access, and misuse. The overcollection and centralisation of sensitive data result in higher stakes and greater potential damage from security failures. The persistent threat of cyberattacks and data misuse undermines the integrity, reliability, and public confidence in national digital services and biometric ID systems. This necessitates a proactive, multi-layered cybersecurity strategy that includes not only robust technological defences but also continuous human capacity-building, stringent ethical guidelines, and rapid, well-resourced incident response protocols.

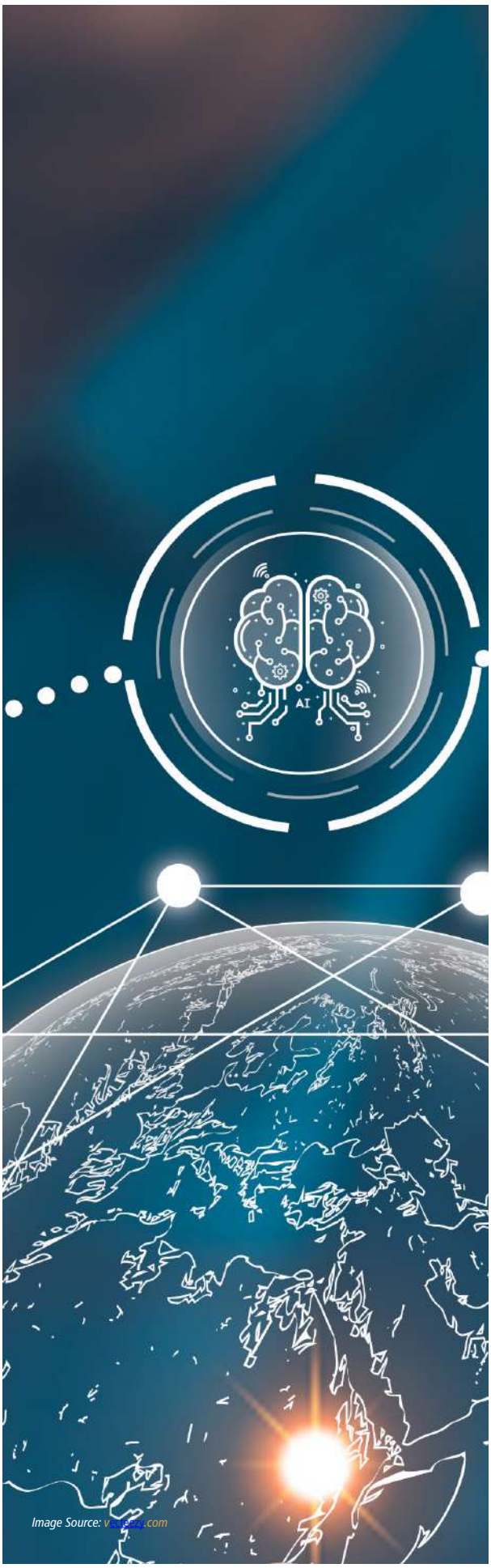

Image Source: v[illegible].com

Image Source: vecteezy.com

PART FIVE

RECOMMENDATIONS AND CONCLUSIONS

5.1 Introduction

As discussed previously in this study, digital identity is the foundation of digital public infrastructure. It is important for governments to get it right at the foundational level for digital services to work. This involves having proper policies in place to anchor digital identity regimes, as well as implementing proper safeguards for data protection and safety. Another key component that often gets overlooked is the training of personnel responsible for implementing these safeguards and policies. There needs to be a concerted effort to build the capacities of both civil society and government actors on the potential harms of not having safeguards from policy level to the roll out.

In addition, this study has pointed out the need to advance responsible, and rights-preserving data systems for digital government services in Kenya and Zambia. While both countries have made concerted efforts to digitise government services, there are persisting gaps and challenges in the rollout and implementation that ought to be addressed, such as legislative reforms and effective implementation of existing laws, inclusion of all individuals and communities, data governance and privacy protection, capacity-building and resource allocation, and collaboration amongst stakeholders.

Thus, this part of the study identifies cross-cutting gaps and challenges impacting the implementation of existing frameworks on government digital services as well as institutional and organisational challenges in the governance of digital services data/biometric ID data in Kenya and Zambia that must be addressed and reformed. In addition, it identifies ways through which governments, private organisations, civil society, and advocacy practitioners in Kenya and Zambia can effectively aid each other in leveraging the delivery of government digital services to the benefit of all. This part of the report proceeds to give recommendations and thereafter, conclusions.

5.2 Recommendations of the Study

The surveys done in Kenya and Zambia sought to understand key areas where the institutions saw the need for improvement in data governance practices for government digital services and biometric ID data. In addition, the second to fourth parts of this study identified areas of concern and challenges impacting the rollout and implementation of digital government services in Kenya and Zambia. The responses to the surveys in Kenya and Zambia and the findings of this study inform the recommendations discussed in this section.

5.2.1 Legislative Reforms and Effective Enforcement

This study noted that there are legislative challenges impacting the rollout of digital ID and government digital services in Kenya and Zambia. Some of the challenges identified in Kenya include inadequate and discriminatory legislation of digital ID, particularly in relation to marginalised groups and people living in remote areas, lack of effective implementation of data protection regulations, insufficient resources and capacity to enforce laws, and political interference in legislation and enforcement. Addressing these challenges will be crucial for Kenya to strengthen its regulatory frameworks, enhance data protection mechanisms, and ensure the effective and responsible implementation of digital ID systems in the country. By overcoming these obstacles, Kenya can better protect individuals' data rights, promote trust in digital ID systems, and foster a more secure and privacy-conscious digital environment.

The surveyed CSOs in Kenya called for stronger enforcement of Kenya's DPA. To address this, CSOs recommend expanding the financial and opera-

tional independence of the ODPC to ensure robust oversight of both government and private-sector data practices. They also noted that establishing clear legal frameworks for data sharing and biometric data governance would play a critical role in strengthening protections for citizens' personal information.

In Zambia, the study identified legislative challenges such as lack of effective enforcement mechanisms, lack of alignment of domestic laws with global standards, and lack of public awareness and education of data protection and privacy laws. Further, CSOs in Zambia noted an urgent need to ensure the full enforcement of existing legal frameworks, particularly the DPA, while also operationalising the Access to Information Act to promote transparency and accountability in public service delivery. Strengthening these legal foundations will provide a critical safeguard for the rights of citizens in the digital age. By tackling these legislative challenges comprehensively, Zambia can strengthen its legal framework, enhance data protection mechanisms, and promote responsible data management practices in the digital era.

Establishment of robust legal frameworks and regulations is essential to safeguard data processing, ensure compliance with data protection laws, and address emerging challenges in digital identity systems. Kenya and Zambia need to refine their legal systems to respond to issues such as data breaches, cybersecurity risks, and human rights violations to facilitate the successful rollout and implementation of digital identity initiatives and digital government services. Both countries also need to effectively enforce existing legislation.

5.2.2 Enhancing Data Governance and Data Protection

This study noted a pervasive lack of transparency in data collection, sharing, and overall governance practices in both Kenya and Zambia. The study also observed that key documents like DPIAs are rarely made public, and there is a consistent lack of clear government communication regarding the purpose of data collection, who controls data, and how it will be stored or shared. Many citizens remain unaware of how their personal information is collected, stored, and shared, or of their fundamental data privacy rights. This points to the need for disclosure of DPIA documents and clear and consistent communication on the collection, storage and transfer of data relating to digital ID and digital government services. On this note, CSOs in Kenya stressed the need for greater transparency in digital ID rollouts, including the public release of DPIAs and the implementation of stronger safeguards against unnecessary biometric data collection.

CSOs in Zambia called for greater clarity and accountability in data collection practices. They noted that government agencies must explain the purposes for which data is gathered, identify data controllers, and put in place meaningful consent processes that uphold individual autonomy. These practices should be complemented by stronger institutional collaboration and the development of interoperable systems that facilitate secure and efficient data exchange across public entities.

Further, CSOs in Zambia stressed the need for clear, well-resourced incident response protocols to address data breaches and governance failures. These mechanisms should include accountability measures and avenues for redress, thereby reinforcing public trust and ensuring that the protection of personal information remains a central pillar of Zambia's digital governance agenda.

In addition, to enhance data governance in Kenya and Zambia, there is a need for stronger cybersecurity enforcement, capacity-building programmes, and increased investment in secure data storage infrastructure. The need to effectively enforce data protection laws cannot be overstated.

5.2.3 Digital Access and Inclusion

In both Kenya and Zambia, there is persistent exclusion of marginalised communities from digital services. Groups such as those in rural areas, refugees, IDPs and stateless persons are victims of such exclusions. It was, for instance, established that limited network coverage, lack of smartphones, and financial constraints disproportionately affect rural and peri-urban populations in both countries. Further, inability to register for and access digital services, stemming from lack of foundational identity documents, perpetuates exclusion from essential services. Therefore, there is a need for practices and policies that allow for digital access and inclusion. Ensuring that all individuals, including those from marginalised communities, have access to identification services is crucial for promoting inclusivity and addressing social disparities. Mandatory requirements for registration and digital ID enrolment should be reviewed to prevent exclusion and restrictions on access to essential public services for vulnerable groups

Addressing challenges relating to exclusion and lack of access requires a holistic approach prioritising digital inclusion, education, and equitable access to technology. Governments and stakeholders must actively work to bridge the knowledge gap, ensure that digital services are designed with inclusivity in mind, and monitor the impact of these platforms to prevent the perpetuation or exacerbation of systemic inequalities in Kenya and Zambia. CSOs in Kenya urged policymakers to adopt a rights-based approach to digital governance, ensuring that no group is excluded due to documentation barriers

5.2.4 Addressing Systemic Inequalities

The study established that gender inequality significantly impacts the effective implementation of digital identification, particularly in Kenya. There were also disparities in mobile phone ownership and usage between genders. Thus, improving female access to mobile technology and enhancing digital literacy could bridge this gap, ensuring more equitable access to digital IDs and associated government and social services. In Zambia, while progress has been made, persistent challenges such as gender disparities and systemic inequalities underscore the necessity for concerted efforts. Inclusive design principles, capacity-building initiatives, and robust regulatory frameworks are essential for ensuring equitable access to digital services and protecting individuals' rights. Moreover, there is a need for increased collaboration between government, private sector, and civil society stakeholders to address the multifaceted challenges in Zambia's identity ecosystem

5.2.5 Building Capacities and Resource Allocation

The study established that limitations in technical infrastructure, human resources, and financial investment consistently hinder the effective implementation of digital governance frameworks and the provision of secure, efficient digital services in both Kenya and Zambia. The study also noted that limited technical infrastructure, particularly in rural and underserved areas, continues to impede secure data transmission and restrict access to government digital platforms.

Private companies in Kenya advocated for increased investments in next-generation cybersecurity infrastructure and for capacity-building initiatives aimed

at improving digital literacy. Such measures, they argue, will create a more predictable and secure environment, thereby fostering innovation while safeguarding consumer rights and data privacy. In addition, building the capacity of government institutions and civil society actors remains a key priority. This includes establishing internal governance frameworks, improving technical infrastructure, and creating sustainable funding mechanisms for training, policy engagement, and monitoring.

In Zambia, investment in digital literacy and rights awareness is essential. CSOs emphasised the importance of targeted outreach campaigns, especially in underserved and rural communities, to build an informed public that can safely and confidently navigate digital services. Such efforts should also extend to training public officials on ethical data handling, inclusive service design, and regulatory compliance.

Increased investments in digital literacy programmes are necessary to empower individuals, enabling them to engage with digital government platforms more effectively.

5.2.6 Improving Collaboration Between CSOs, Private Sector and Government Agencies

Improving collaboration between CSOs and government agencies is seen as essential for refining digital service frameworks. Continuous dialogue between policymakers and civil society actors is crucial in this context, as it can help ensure that digital governance strategies are inclusive and responsive to the needs of all citizens.

Industry respondents in Kenya called for enhanced public–private collaboration to resolve regulatory ambiguities and improve cybersecurity practices. They recommended that regulators engage more proactively with industry stakeholders to establish clear, consistent guidelines for data-sharing and biometric data management. In Zambia, CSOs suggest that they should be formally integrated into regulatory and policy development processes to ensure inclusive, rights-based approaches to digital transformation.

5.2.7 Ethical Guidelines for Digital Technologies

To ensure the responsible deployment of biometric and digital ID systems, governments in Kenya and Zambia should empower their respective data protection agencies to lead the development of ethical guidelines for digital technologies. These agencies' regulatory mandates and expertise in enforcing data protection laws position them well to address key concerns such as informed consent, data minimisation, and safeguards against misuse. However, their primary focus on legal compliance may limit their capacity to address broader ethical challenges, such as the societal implications of surveillance, exclusion, or algorithmic bias in biometric systems. To bridge this gap, their efforts should be complemented by independent ethics panels composed of experts in technology, ethics and human rights. This collaborative structure would help ensure that the resulting guidelines are both technically sound and ethically grounded. The guidelines should mandate transparency in data practices, prohibit discriminatory applications, and establish safeguards against risks such as mass surveillance or unauthorised data sharing. By allowing data protection agencies to take the lead while incorporating diverse perspectives, this approach can enhance public trust and support rights-based digital governance.

5.2.8 Decentralised Citizen Feedback and Redress Mechanism

To strengthen accountability and cultivate trust in digital governance in both Kenya and Zambia, a robust, multi-faceted approach is essential, emphasising community-led monitoring initiatives and establishing secure anonymous reporting channels. Community-led monitoring involves empowering local civil society organisations and community groups to act as independent observers of government digital service delivery and digital ID implementation. By actively engaging with citizens, particularly in underserved areas, these initiatives facilitate the collection of grassroots feedback, ensuring policies and their implementation are responsive to community needs and helping identify critical insights and challenges directly from the ground.

Parallel to this, the establishment of genuinely secure and accessible anonymous reporting channels is vital. These dedicated mechanisms enable both citizens and public servants to confidentially report concerns such as data breaches, instances of corruption in digital service provision, or observed infringements of digital rights. The assurance of anonymity is key to encouraging the disclosure of sensitive information and malpractices that might otherwise go unaddressed, thereby promoting transparency and accountability. Finally, it is essential to have ongoing public awareness campaigns that empower people to exercise their rights and pursue redress when necessary. These campaigns should clearly explain, through various media platforms, what rights citizens have when using government digital services and digital ID systems. They should also outline the formal channels available for submitting complaints, providing feedback, or seeking appropriate remedies. Equipping people with this information strengthens public confidence in digital systems and ensures that digital transformation remains responsive to the needs and realities of everyday citizens.

5.2.9 Advancing Interoperability for Inclusive Digital Services

To fully realise the benefits of digital ID systems and government digital services in Kenya and Zambia, it is essential to prioritise the development of strong interoperability frameworks. This absence of coordinated effort and frictionless data exchange among government agencies frequently manifests as fragmented service delivery, leading to the cumbersome re-collection of information and an often-frustrating user experience across public services. These silos limit governments' ability to build a holistic view of citizen needs and hinder efficient access to services, especially for marginalised populations. A shift toward integrated digital infrastructure, where systems can securely and reliably communicate, is necessary to streamline operations, reduce administrative burdens, and improve public service delivery across sectors.

To achieve this, both technical and institutional reforms are required. First, both countries should invest in standardising data formats and adopting secure data exchange protocols. This will ensure that platforms supporting civil registration, taxation, and health services, among others, can communicate and operate in harmony. Additionally, these technical measures should be reinforced through clear legal and policy frameworks that outline how data is shared, who is accountable, and what safeguards must be in place. Importantly, privacy, security, and informed consent should be embedded as foundational principles in all data-sharing practices. Finally, a designated oversight body should be tasked with coordinating interoperability efforts, resolving implementation challenges, and monitoring compliance across institutions. By adopting this

approach, both countries can build inclusive and efficient digital ecosystems that offer coherent, user-friendly services to all citizens.

5.3 Key Takeaways from the Study

This study has established that both Kenya and Zambia have and continue to digitalise government services. A mapping of digital government services in both countries identified digitised services such as tax payments, business registration, transport management, healthcare, civil registration, government procurement and land administration, amongst others. Some of the notable platforms and initiatives in Kenya include eCitizen, Huduma Kenya services, Gava Mkononi, iTax, e-Justice system, and IFMIS, among others. In Zambia, initiatives such as Smart Village, Digital Zambia Acceleration Project, and Digital Public Service Transformation exist. Kenya and Zambia are also actively developing their digital identity infrastructures.

While government digital services are valuable for addressing social challenges and developing solutions, the digitalisation of government services introduces new challenges. These include cybersecurity and data privacy concerns arising from increased collection and centralisation of sensitive personal information, legislative challenges resulting from ineffective enforcement of and gaps in existing legislation, gender and systemic inequalities, exclusion of individuals and communities from access to digital IDs and digital services, and lack of community engagement.

Surveys conducted with relevant stakeholders in government, private sector, and CSOs in Kenya and Zambia identified challenges relating to roll out of digital government services and implementation of existing frameworks. The participants noted challenges such as lack of digital access and exclusion resulting from exclusion of marginalised communities, limited digital literacy, the lack of proper identification, and inadequate infrastructure in remote areas; biometric ID implementation and governance concerns resulting from exclusion from biometric data due to technical errors and lack of transparency around how sensitive biometric data is collected, stored, and shared; data governance and privacy protection deficits resulting from over-collection and centralisation of biometric data without clear justification or safeguards, along with opaque data-sharing practices across government agencies; ineffective regulatory frameworks resulting from weak enforcement, regulatory gaps, limited transparency in government data practices such as the non-disclosure of data protection impact assessments in Kenya, and insufficient public participation; and capacity and resource constraints resulting from limitations in technical infrastructure, human resources, and financial investment.

Building on the identified gaps and challenges, the study calls for legislative reforms and enforcement; enhanced data governance and data protection through stronger cybersecurity enforcement, capacity-building programs, increased investment in secure data storage infrastructure and continuous compliance with data protection laws; practices and policies that allow for digital access and inclusion; addressing systemic inequalities; building capacities and resource allocation; improving collaboration among stakeholders; empowering data protection agencies to lead the development of ethical guidelines for digital technologies; decentralising citizen feedback and redress mechanisms; and advancing interoperability for inclusive digital services.

5.4 Conclusions

Digital government services platforms and initiatives play a vital role in enhancing efficiency, transparency and access to government services. They also foster economic growth and transform the way governments operate and interact with the people and entities.

While both countries have made concerted efforts to digitise government services, there are persisting gaps and challenges in the rollout and implementation that ought to be addressed. It is also important for governments to get digital identity right at the foundational level for digital services to work by having proper policies in place to anchor digital identity regimes and implementing proper safeguards for data protection and safety.

Finally, it takes a multi-stakeholder approach to fully address the gaps and challenges impacting the implementation of existing frameworks on government digital services as well as institutional and organisational challenges in the governance of digital services data/biometric ID data in Kenya and Zambia.

This study was made possible by a grant provided by the International Development Research Center (IDRC). We thank the organization for their continued support.

Canada

Supported by

Ole Sangale Rd, Madaraka Estate.
P.O Box 59857-00200, Nairobi, Kenya.
Tel: +254 (0)703 034612
Email: cipit@strathmore.edu
Website: www.cipit.strathmore.edu