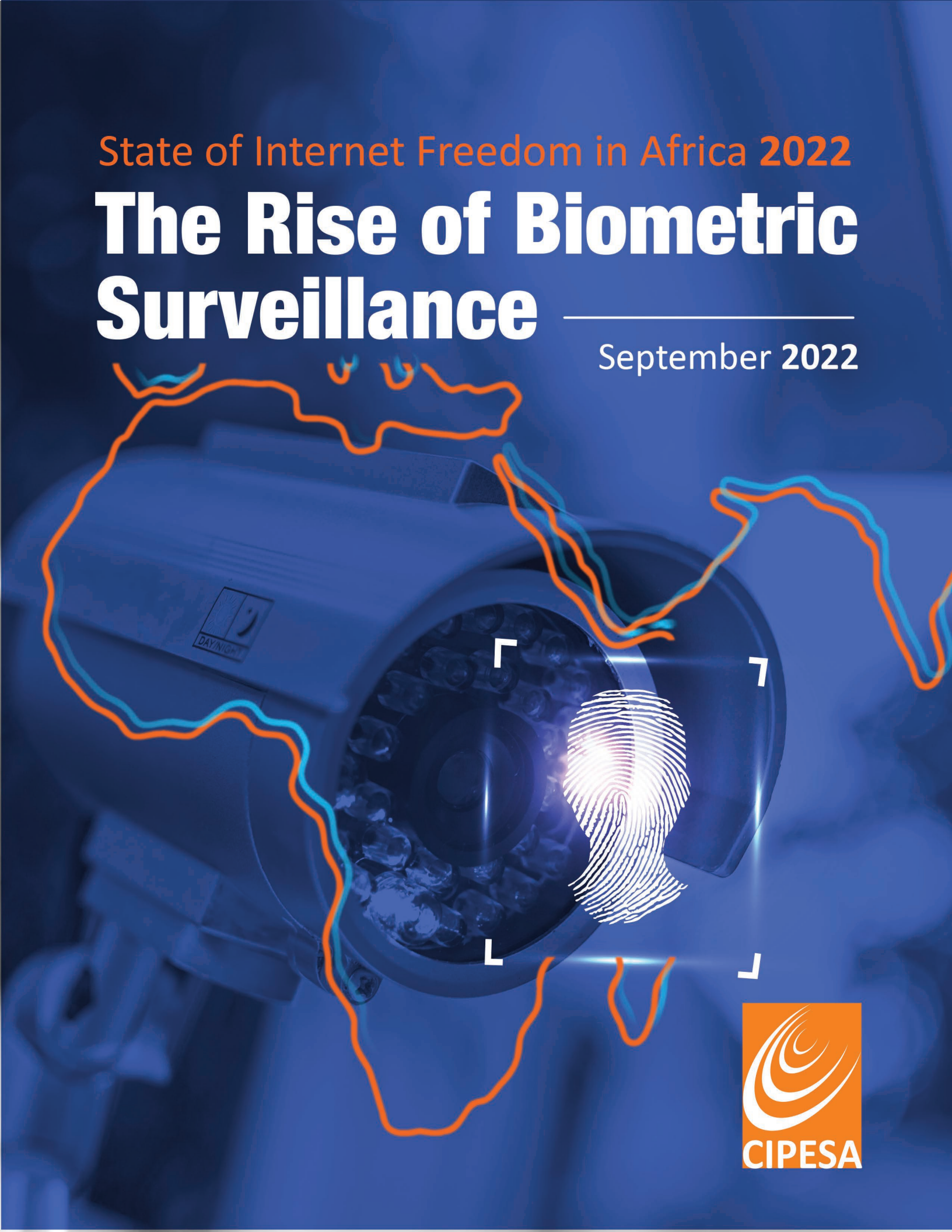
State of Internet Freedom in Africa **2022**

The Rise of Biometric Surveillance

September **2022**



CIPESA

Table of Contents

1.0 Introduction

Technologies including biometric systems present new opportunities and challenges to privacy, freedom of expression, access to information, equality and non-discrimination. Biometrics refers to the measurement and analysis of physical or behavioural characteristics such as blood types, fingerprints, deoxyribonucleic acid (DNA), retinal pattern, facial thermogram, hand geometry, and voice to verify a person's identity.[1] These characteristics are often linked with other personal biographical information in databases containing individuals' names, contact information, demographic characteristics, medical history, opinions, and correspondence. Once consolidated, the databases can be used in various ways to facilitate service delivery through applications in areas such as digital identification and verification, voter registration and identification,[2] SIM-card registration, issuance of driver's licenses, COVID-19 surveillance, financial transactions and payments, social protection, refugee services, passport and visa issuance, border control, traffic control, healthcare provision, migration management,[3] and access control for devices, systems and premises.

The right to privacy is recognised in several regional and international human rights instruments and is guaranteed in the national constitutions of many African states. One such instrument is the 2019 African Commission on Human and Peoples' Rights (ACHPR) Declaration on Principles of Freedom of Expression and Access to Information in Africa, which provides in Principle 40 that "Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information." The Declaration, further calls upon African Union Member States, in its principle 42, to among others, adopt laws for the protection of personal information of individuals in accordance with international human rights law and standards that provide for privacy principles, effective remedies, and adequate oversight. There have been deliberate efforts by states to comply with the established standards. However, challenges remain as state and non-state actors grapple with designing and implementing biometric technology-based programmes.

This report documents the emerging and current trends in biometric data collection and processing in Africa. It focuses on the deployment of national biometric technology-based programmes on the continent, and the associated challenges, gaps and risks that are posed to data protection and privacy.

1 *See for example, the Free Dictionary, "biometrics," https://www.thefreedictionary.com/biometrics*

2 *Introducing Biometric Technology in Elections https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf*

3 *IOM and Biometrics https://www.iom.int/sites/g/files/tmzbdl486/files/our_work/DMM/IBM/iom_and_biometrics_external_info_sheet_november_2018.pdf*

1.1 Background to the Study

Digital biometric data collection programmes are becoming increasingly popular across the continent.[4] Governments are investing in diverse digital programmes[5] to enable the capture of biometric information of their citizens for various purposes. Indeed, these programmes have gained momentum and have been hailed as key enablers of development. They are also expected to fast-track the recognition and registration of 494 million people in Sub-Saharan Africa who form 45 per cent of people worldwide who do not have any form of official proof of legal identity.[6]

Digital IDs are progressively replacing the old paper-based identity documents. Digital IDs are taking the form of smartphone applications or smart cards which utilise technologies such as Bluetooth, Near-field communication (NFC),[7] Radio-frequency identification (RFID),[8] blockchain technology,[9] and Public Key Infrastructure.[10] They have the potential to provide timely, efficient and secure solutions for authorities that issue them and their ability to interface with other systems and databases is another advantage. They are being applied in different ways for government services and consumer and commercial applications across different sectors.

As of 2021, 136 countries had implemented digital ID programmes which amount to 3.6 billion digital IDs in circulation.[11] Further, 82% of all countries issuing national IDs have implemented digital ID programmes that depend on digital ID chip cards or plastic cards and biometrics. This demand has created a global market for digital ID which has increased from USD 18 billion in 2018 to USD 44.7 billion in 2022, according to Acuity Market Intelligence, with the size of the market for biometric and digital identity documents in Africa estimated at USD 1.4 billion.[12]

The COVID-19 pandemic heightened[13] the need to prove identity and at the same time enhanced the use of new contactless biometric technologies such as facial recognition and iris scans, as people avoided biometric devices requiring contacts such as palm print, fingerprint, and hand-key readers, which accelerated digital transformation in several countries. Likewise, the rising smartphone access, mobile telephone coverage and internet penetration rates on the continent are key drivers for biometric programmes, with an additional 120 million new subscribers expected within Sub-Saharan Africa by 2025, up from 495 million recorded in December 2020.[14] Mobile technologies and services are expected to generate USD 155 billion of economic value by 2025, up from 130 billion recorded in 2020.

Proponents of biometric data collection such as governments, the African Union (AU), the World Bank, Non-Governmental Organisations (NGOs) and the private sector players such as banking, telecoms and security sector, state that such systems are important to accurately identify, authenticate and verify the identity of individuals, including by facilitating know-your-customer (KYC)[15] requirements; ensure the provision of legal identity in line with Sustainable Development Goal (SDG) 16.9; promote national security; strengthen democracy[16] and election integrity;[17] prevent financial, identity fraud, identity theft; combat corruption; and counter-terrorism.

4 *Biometric data: 100 countries ranked by how they're collecting it and what they're doing with it https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/*
5 *Biometrics: Friend or foe of privacy? https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf*
6 *Global Identification Challenge by the Numbers https://id4d.worldbank.org/global-dataset/visualization*
7 *Near-field communication is a set of communication protocols that enables communication between two electronic devices over a distance of 4 cm or less. https://developer.android.com/guide/topics/connectivity/nfc*
8 *Radio-frequency identification uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter. https://www.abr.com/what-is-rfid-how-does-rfid-work/*
9 *Blockchain technology allows for users to create and manage digital identities through the combination of the following decentralized identifiers, identity management and embedded encryption. https://consensys.net/blockchain-use-cases/digital-identity/*
10 *The Public key infrastructure (PKI) is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-keys. PKIs are the foundation that enables the use of technologies, such as digital signatures and encryption, across large user populations. https://bit.ly/3Cdbolx*
11 *Global Identification Challenge by the Numbers https://id4d.worldbank.org/global-dataset/visualization*
12 *Biometric identification: a coveted African market https://www.theafricareport.com/30838/biometric-identification-a-coveted-african-market/*
13 *Challenges of Fingerprinting: Will Digital IDs Revolutionise Service Delivery in Sub-Saharan Africa? https://africanarguments.org/2022/03/challenges-of-fingerprinting-will-digital-ids-revolutionise-service-delivery-in-sub-saharan-africa/*
14 *The Mobile Economy Sub-Saharan Africa 2021 https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf*
15 *Reimagining identity ecosystems in Sub-Saharan Africa with mobile https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/12/Reimagining-identity-ecosystems-in-Sub-Saharan-Africa-with-mobile.pdf*
16 *Biometrics: Friend or foe of privacy? https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf*
17 *Biometric Technologies and The Prospect of Sustainable Democracy in Africa https://eisa.org/pdf/JAE20.1Idowu.pdf*

Further, proponents say these systems enhance trust and confidence in identification and payment systems; improve financial sector services; facilitate efficient delivery of social services including e-health, aid delivery and social protection programmes; enhance the quality of data by eliminating the duplication of records; control physical and digital access to premises and digital systems; improve data security; link databases to improve monitoring and feedback systems; and support the growth of the digital economy.

Unfortunately, these programmes also present new risks to the realisation and enjoyment of human rights and freedoms. These programmes require the mandatory collection and processing of sensitive personal data of millions of citizens, and the protection of the privacy of this data from a technical, legal, regulatory and procedural perspective is critical. Notably, the programmes, such as the issuance of ePassports by almost 50 African nations,[18] have been implemented amidst a deficiency of comprehensive data protection laws,[19] adequate protection[20] or remedies and independent oversight institutions. Just over half of the countries on the continent have specific data protection frameworks. This is compounded by the absence of effective and robust safeguards against data privacy abuse, especially in countries where surveillance by state security agencies remains poorly regulated with no clear audit processes and enforcement mechanisms. There are also no clear strategic approaches to rolling out data protection and security programmes, which has led to a crowded and disorganised identity management ecosystem.[21]

Further, incomprehensively implemented biometric digital ID programmes could entrench digital exclusion and discrimination of vulnerable groups from accessing government services. In addition, centralised biometric databases potentially face increased cybersecurity risks and are vulnerable to attacks and loss[22] yet biometrics cannot be easily replaced like passwords and tokens. Moreover, there are concerns relating to the roles and responsibilities of the intermediaries involved in the design, deployment and implementation of these biometric systems, some of which are using African countries as a data harvesting and testing ground[23] for their emerging big data technologies developed outside the continent. Biometric systems with facial recognition capability[24] can be passively used for surveillance, thereby eliminating the requirement for consent, and thus used without the knowledge or participation of the data subject.

1.2 Study Methodology

This study reviews the implementation of select national biometric programmes in 16 African countries including Angola, Cameroon, Central African Republic, Democratic Republic of Congo, Kenya, Lesotho, Liberia, Mozambique, Nigeria, Senegal, Sierra Leone, Tanzania, Togo, Tunisia, Uganda, and Zambia. The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. Reports of previous studies, media reports, academic works, government documents, and other literature were also reviewed. The literature review helped the researchers to gain a better understanding of the current developments, benefits, gaps, challenges, debates and issues on biometric programmes and privacy and data protection in the focus countries.

The legal and policy analysis included a review of laws, policies and practices relating to biometrics and privacy rights. The study also reviewed the progress of select national biometric programmes, including those implemented by non-state actors that present significant privacy risks and recommendations to various stakeholders.

Key Informant Interviews (KIIs) were conducted with purposely selected respondents who were conversant with the issues at hand. They included women rights advocates, staff of private companies, government ministries, telecoms regulators, media houses and consumers' associations. In addition, academics, lawyers and social media users were interviewed.

18 *African countries embracing biometrics, digital IDs https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids*

19 *Mapping and Analysing Privacy Laws and Policies in Africa https://cipesa.org/?wpfb_dl=454*

20 *Activists sound alarm over African biometric ID projects https://www.aljazeera.com/economy/2020/12/10/activists-sound-alarm-over-african-biometric-id-projects*

21 *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa https://www.ictworks.org/wp-content/uploads/2022/01/digital-id-african-country.pdf*

22 *Protection of Personal Information in South Africa: A Framework for Biometric Data Collection Security https://www.thinkmind.org/articles/internet_2016_1_10_40022.pdf*

23 *Who's watching who? Biometric surveillance in Kenya and South Africa https://enact-africa.s3.amazonaws.com/site/uploads/2020-11-11-biometrics-research-paper.pdf*

24 *Collection of Biometric Data and Facial Recognition https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/collection-of-biometric-data-and-facial-recognition/*

2.0 Results: Trends in Adoption of Biometrics Data Collection

This section presents the results of the research. It reviews the different laws and policies that affect biometric data collection. It also examines the various biometric data collection programmes being implemented in the countries studied. Across the different countries, the prevalent biometric programmes include those related to civil registrations, such as for the issuance of National Identity cards, biometric voter registration and identification programmes, government-led CCTV programmes with facial recognition capabilities, national ePassport initiatives, refugees' registration, and mandatory biometric SIM card registration.

2.1 Legal Framework on Biometrics

The national constitutions of the countries studied guarantee the protection of the right to privacy including personal data. At least 30 countries across the continent have, in addition to the constitutional provisions, enacted laws and policies to provide for data protection.[25] However, several countries have legal provisions that legitimise the biometric data collection and processing programs such as SIM card registration, voter registration, and national identification.[26]

The main enabling laws for biometric data collection in the countries studied include those on civil registration, immigration, elections, financial services and telecommunication. These laws, especially in Angola, Cameroon, Central African Republic, Democratic Republic of Congo, Kenya, Lesotho, Liberia, Mozambique, Nigeria, Senegal, Sierra Leone, Tanzania, Togo, Tunisia, Uganda, and Zambia, enable the collection of fingerprints, photos and signatures before official documents such as IDs and passport are issued. In other countries like Kenya, Nigeria and Zambia also mandate iris scans.

In addition, the countries studied also use the established national identification authorities as a means to collect biometric data before national identity cards are issued. In Sierra Leone, additional types of information which the law says should be collected include those relating to the blood group, eye colour and height. On the other hand, Uganda is in the process of implementing an upgrade of the national identification system to include DNA, palm print and eye scan data to the details of the individual in the national register. A law requiring the collection of DNA and GPS coordinates for identity registration in Kenya was declared unconstitutional. Furthermore, the laws on electoral processes have been widely used to collect data including photos and fingerprints for purposes of identifying voters, and are in some cases linked with data from official civil registration databases such as digital IDs and passports, which are often required for voters' registration.

25 Olumide Babalola, "Data Protection Legal Regime and Data Governance in Africa: An Overview, 2022," https://www.africaportal.org/documents/22659/DG003.pdf

26 For a detailed analysis of the different privacy and data protection laws including on biometrics, please see CIPESA's 2022 report; Privacy Imperiled: An analysis of Surveillance, Encryption and Data Localisation Laws in Africa https://cipesa.org/?wpfb_dl=492

While there has been a mass collection of biometric data using different laws, the protection of the data is sufficient. In some countries, there are no data protection laws. In others, the laws are weak as they fail to outline the objectives of the collection, specify the legitimate uses of the data, control access to the data, build in risk management, or provide transparency and accountability mechanisms. In turn, such laws tend to facilitate access to the data without sufficient safeguards. The laws such as Law No. 18-07 of 2018 on the protection of personal data for Algeria,[27] Kenya's Data Protection Act 2019,[28] Angola's Data Protection Act of 2011, Ivory Coast's Data Protection Law of 2013 and Uganda's Data Protection and Privacy Act 2019[29] provide for circumstances under which personal data including sensitive information may be processed. These provisions give leeway for easy access and processing of personal data.

The laws prescribe ways through which personal data may be processed especially in the interest of national security, public interest, enforcement of the law and conduct of criminal investigations. Unfortunately, the scope and limits within which data may be processed are not succinct. They also lack clear checks against possible data privacy violations and tend to lean towards facilitating access by the state and its agencies as opposed to protecting the rights of data subjects. It is also commonplace in some of the countries studied to find that the laws are largely used to ease access to the personal data of individuals to identify and target them. The main categories of targeted individuals include human rights defenders, political activists, dissidents and government opposition actors.

The UN 2018 Addendum to the 2015 Security Council (Madrid) Guiding Principles on Foreign Terrorist Fighters[30] notes that biometric technology creates challenges because of the gap that exists between technological innovation and the introduction of legislation regulating such technology. Consequently, States are called upon to consider introducing effective privacy impact assessments or establishing review or other types of oversight bodies, to anticipate and consider the potential impact of such new technologies or applications. Additionally, states are required to ensure that any interference with privacy must comply with international human rights law, which prohibits arbitrary or unlawful interference with privacy.

Article 10(4) of the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)[31] calls upon states to only engage in the processing of personal data involving biometric data after authorisation by the relevant protection authority. As discussed further in this report, several countries have engaged in the collection and processing of biometrics without adequate legal, technical or regulatory safeguards, such as the establishment of independent data protection bodies. In any case, only a quarter of all African countries (14) have signed the convention with less than 25% (13) having ratified it.[32]

Among the study countries, only Mozambique, Sierra Leone, Togo, Tunisia, and Zambia have signed the Convention, while only Mozambique, Senegal, Togo, and Zambia have deposited the instruments of ratification. The rest of the countries in the study, namely Angola, Cameroon, Central African Republic, Democratic Republic of Congo, Kenya, Lesotho, Liberia, Nigeria, Tanzania, and Uganda are yet to sign or ratify the convention. Senegal and Tunisia, who have made moves towards endorsing the Malabo Convention, are also members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty No. 108).[33]

27 *Article 18*

28 *Part V (section 44-47)*

29 *section 9*

30 *Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-on-foreign-terrorist-fighters.pdf*

31 *AU Convention on Cybercrimes and Personal Data Protection https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf*

32 *Status List https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf*

33 *Chart of signatures and ratifications of Treaty 108 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108*

2.2 Biometric data collection programmes

2.2.1 Civil Registrations, including the issuance of National Identity Cards

Although not widespread, several countries have adopted the use of biometrics such as fingerprint, facial or iris recognition as a form of authentication for purposes of issuing birth and national identity cards.[34] The African Union's Digital Transformation Strategy for Africa (2020-2030) recognises the importance of digital ID in promoting trust which is critical for the continents digital economy and the establishment of the digital single market in line with the Africa Continental Free Trade Agreement (AfCFTA). It proposes to ensure inclusion, security, privacy and data ownership in digital identity systems, and to support the interoperability and neutrality of digital identity systems as part of its transformation agenda.[35] A Pan-african digital ID could mirror or be informed by the proposed digital ID wallet currently being developed by the European Union.[36] The EU has been instrumental in shaping the AU's digital transformation efforts,[37] and supporting the roll-out of digital identification programmes in several countries in West Africa.[38]

In 2016, the Economic Community of West African States (ECOWAS) launched the ECOWAS Card as a standard biometric identity card for citizens of its member states. The card can also be used as a travel document for residents and replaces the resident permits used within its 15 Member States. The implementation of this initiative requires the establishment of foundational identity databases to serve as a reliable reference for other services such as the issuance of passports, driver's licences, voter's cards and social security cards.[40]

Beyond ECOWAS, various countries have also initiated biometric data collection, including for national IDs, voters' registration and other purposes. In Angola, the government has since 2009 been issuing the 10 years validity digital IDs to its citizens. This ID system was designed to safeguard personal data while also storing substantial amounts of biometric information directly on the card, including two thumb fingerprints and iris images, a birth certificate, and demographic data.[41]

In Cameroon, there have been multiple identity programmes, but none have been sustainable or robust. In 1994, the government worked with a private entity to register individuals and issue national identity (NID) cards and residence permits. In 2005, the processing of biometric data started. In 2008, the NID was upgraded to include a colour photo and electronic fingerprint of the cardholder, along with additional security features, and in 2013, the government started issuing electronic NID. These electronic IDs were meant to be used for multiple electronic services such as civil identification and health and social services.[42] In the Central African Republic, there have been reports in 2020 of discussions between the government and Securiport, a private firm, to launch biometric identification and delivery of electronic IDs to all citizens and refugees.[43]

In 2019, Kenya launched the National Integrated Identity Management System (NIIMS) also known as Huduma Namba (Swahili translation for 'service number').[44] As part of the registration for the Huduma Namba digital ID in 2019, the public was required to present all their personal documentation such as national identity cards, birth

34 *African countries embracing biometrics, digital IDs https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids*

35 *African Union's Digital Transformation Strategy for Africa (2020 - 2030) https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf*

36 *European Digital Identity https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en*

37 *Africa https://digital-strategy.ec.europa.eu/en/policies/africa; Towards a EU-Africa Digital Partnership https://ec.europa.eu/futurium/en/eu-au-digital-economy-task-force/towards-eu-africa-digital-partnership-0.html*

38 *Digital4Development: mainstreaming digital technologies and services into EU Development Policy https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2017)157&lang=en*

39 *The ECOWAS Card: converting a challenge into an opportunity https://peopleid.zetes.com/sites/default/files/br_cedeao_20161110_uk_4.pdf*

40 *Link project to civil register https://peopleid.zetes.com/en/link-project-civil-register*

41 *The state of identification systems in Africa: country briefs (English). Washington, D.C: World Bank Group. https://bit.ly/3SzOqdE*

42 *Ibid Cross ref 37*

43 *Biometrics and digital ID in Africa: GenKey in Niger, Securiport in CAR, new reseller partner for Daon in SA https://bit.ly/3dNRPqo; Conference proposes biometrics-based documentation for Central African Republic refugees, https://bit.ly/3CeJjdx*

44 *Africa: regulate surveillance technologies and personal data https://www.nature.com/articles/d41586-022-01949-9*

certificates, birth notifications, National Health Insurance Fund (NHIF) cards, National Social Security Fund (NSSF) cards, Kenya Revenue Authority Personal Identification Number (PIN) certificates, driver's licence, alien identification cards, refugee identification cards, passports, disability cards, and National Education Management Information System (NEMIS) cards.[45]

The biometric technology-based system was a mysterious, far-reaching and compulsory data collection project that aimed to create a 'single source of truth' of all information about citizens and foreign nationals in the country. It also sought to consolidate information from other databases such as national identity cards, passports, driver's licenses, social security, and national health insurance. Despite its implementation in the absence of a comprehensive legal framework, the KES 9.6 billion (USD 79.7 million) project was halted by courts[46] after collecting personal data of 37 million people in its first phase and processing five million cards by June 2021.[47]

Lesotho's national biometric digital identity cards were introduced[48] in 2013 and have covered 85% of the eligible population.[49] Obtaining the national ID is integrated with the birth and death registration processes. The birth certificate is required as part of the application for the NID. A photo and fingerprints from all 10 fingers are taken digitally. After an online deduplication check confirms that the individual has not already been enrolled, a 2-D barcode credential is printed. It contains a machine-readable fingerprint and biographical information as well as a photo and other information on the face of the card.

In Liberia, the National Identification Registry (NIR) was established by law in 2011 and authorised to implement the National Biometric Identification System (NBIS).[50] Howeer, the government only set up a management team and allocated provisional funding for the NIR in October 2015. The NIR hopes to establish or acquire the technical infrastructure and control procedures that will serve as the platform for the implementation of the NBIS. This system whose pilot commenced in November 2021[51] is expected to collect, organise, store, secure, and grant access to secure biometric data collected from individuals applying for national biometric identification cards and other key documents, such as passports, driver's licenses, and social security cards. Liberia has multiple functional identity systems, including passport numbers, civil servant registration numbers, social security numbers, driver's license numbers, birth registration numbers, and voter registration. Some of these systems capture biometric information.[52]

Mozambique implements[53] a digital ID card with a Unique Citizen Identification Number (NUIC), the National Immigration Service (SENAMI), for its immigration system for travel documents and residence permits; and the Electronic System for Civil Registration and Vital Statistics (e-SIRCEV) system for civil registration established in 2018.[54] Mozambique has a unique national identification number, assigned during birth registration. This national identification number is used on NID cards, health cards, driver's licenses, and passports. Birth certificates are a prerequisite for obtaining NIDs. The NID is valid for five years for individuals below 40 years of age and valid for 10 years for individuals between aged between 40 and 50 years. The card is valid for life if the cardholder is over 50. The NID is mandatory and is regulated by Decree no 11/2008 of the Council of Ministers. Mozambique's NID is a laminated card with a magnetic strip that contains an ID number, photograph, full name, sex, date of birth, nationality, address, biometrics (fingerprints), place and date of issue, height, occupation, marital status, expiration date, and signature of the user. Mozambique does not have stand-alone legislation on personal data protection.[55]

45 *Huduma Namba digital capture form https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/form-hn-23-Data-Capture-Tools-14-3-2019.pdf; Huduma Namba Regulations 2021, https://ict.go.ke/wp-content/uploads/2020/10/HUDUMA-NAMBA-REGULATIONS-2020.2021.pdf*

46 *Why the Huduma Namba ruling matters for the future of digital ID, and not just in Kenya https://privacyinternational.org/news-analysis/3350/why-huduma-namba-ruling-matters-future-digital-id-and-not-just-kenya*

47 *State banks on new portal to ease collection of Huduma cards https://nation.africa/kenya/news/state-banks-portal-to-ease-collection-of-huduma-cards-3439902*

48 *State of Digital Identity in Lesotho https://researchictafrica.net/wp/wp-content/uploads/2021/11/Lesotho_31.10.21.pdf*

49 *Lesotho Digital Economy Diagnostic https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y*

50 *Identification for Development (ID4D) Identifi cation Systems Analysis Liberia Country Assessment https://openknowledge.worldbank.org/bitstream/handle/10986/26438/113549-WP-P156810-PUBLIC-Liberia-ID4D-Web.pdf?sequence=1&isAllowed=y*

51 *Liberia: National Identification Registry to Issue National ID Cards to Liberians along Sierra Leone Border https://citizenshiprightsafrica.org/liberia-national-identification-registry-to-issue-national-id-cards-to-liberians-along-sierra-leone-border/*

52 *Ibid cross ref 37*

53 *Digital Identify in Mozambique https://researchictafrica.net/wp/wp-content/uploads/2021/11/Mozambique_3.11.21.pdf*

54 *Ibid cross ref 50*

55 *Ibid cross ref 37*

In Nigeria, the National Identity Number (NIN) is an 11-digit random unique number assigned to an individual for life upon successful enrolment in the NID database. The NID card is a microprocessor chip–based general multipurpose ID card, with 13 applications including ID verification, authentication, and payment technology to help promote financial inclusion. The ID card contains two photographs of the holder and a chip storing an individual's biometric information (10 fingerprints and an iris scan). Biometric deduplication is carried out before NIN issuance. After successful deduplication, a unique NIN is issued and stored in the NID database. Children below the age of 16 are required to register their biometric information with the NIMC and update it every two years. However, the child's biometric information is not used for deduplication. The child is issued a NIN linked to that of the parent.[56] The national biometric identification programme may ultimately cost USD 2.3 billion,[57] in a country where, as of March 2020, only 9% of the nationals had a National Identification Number (NIN), and less than 1% had a national ID card.[58]

In 2005, the Senegalese government announced the digital national ID cards project for all citizens. In the same year, 174 registration centres were set up across the country. To date, at least 67% of the population has either a national ID or a voter ID which are used for civil, social security and voting purposes. The Senegalese ID has a barcode with biometric information along with biographic information. The electronic ID is used for multiple e-services.[59] In 2019, the government embarked on the process of digitising its civil status and national biometric identity file. The project was supported by the European Union under the Support Programme for the Strengthening of the Civil Status Information System and the Consolidation of a National Biometric Identity File in Senegal.[60]

In Sierra Leone, section 37 of the National Civil Registration Act 2016 authorises the National Civil Registration Authority (NCRA) to undertake compulsory and continuous registration of citizens and non-citizens and to collect vital statistics, to establish and maintain an electronic registration system. The system is designed by the law to collect and maintain biometric details of citizens as well as generate a national identification number (NIN). Biometric details of individuals can include the face, fingerprint, blood group, eye colour, and height. However, while the law empowers the NCRA to collect biometric data during the registration process, no such collection happens or has ever happened due to a lack of institutional capacity to roll out such an undertaking. Since 2016, NCRA has been collecting biometric details of Sierra Leoneans to develop a permanent civil register for the country. The last large-scale exercise was done between May and July 2021. From June 2022, all foreign nationals applying for residence and work permits from the government are required to have a national identification number (NIN).[61]

In Tanzania, the government introduced a biometric national ID programme in 2013 and started issuing cards in 2016.[62] As of 2020, at least 22.1 million individuals or 80% of the adult population had registered for the National Identification Number (NIN).[63] Also, mandatory SIM card registration requires the collection of fingerprint data in addition to official documentation such as national identity cards, birth certificates, driver's licenses or passports.[64]

In Togo, although civil registration (registration of births, deaths and marriages) is not yet digitised, recent reports indicate that the digitisation will be done alongside the new biometric national ID which is still in progress.[65] The country announced its e-ID biometric identification programme in 2018, and plans are underway to roll out the project to provide identity cards to the entire population since only 25% of the population have IDs.[66]

56 *Ibid cross ref 37*

57 *Biometrics and digital ID across Africa this week: savings and costs in Nigeria, divisions in Tanzania, Ghana https://www.biometricupdate.com/202003/biometrics-and-digital-id-across-africa-this-week-savings-and-costs-in-nigeria-divisions-in-tanzania-and-ghana*

58 *Biometrics and digital ID across Africa this week: savings and costs in Nigeria, divisions in Tanzania, Ghana https://www.biometricupdate.com/202003/biometrics-and-digital-id-across-africa-this-week-savings-and-costs-in-nigeria-divisions-in-tanzania-and-ghana*

59 *The World Bank (2017) The State of Identification Systems in Africa, https://tinyurl.com/wfvhjfd*

60 *Computerization of civil status and the national biometric identity file: Oumar Guèye in "fast track" mode: https://bit.ly/3w1yZSQ; Civil status: the lack of statistics on births noted https://senegalservices.sn/actualite/etat-civil-le-deficit-de-statistiques-sur-les-naissances-releve*

61 *Digital ID needed for passport, residence, work permits in Sierra Leone https://www.biometricupdate.com/202205/digital-id-needed-for-passport-residence-work-permits-in-sierra-leone*

62 *Report on the Community of Practice on the Digital Enquirer Kit https://www.africaportal.org/features/tanzania-nida-ids-civic-services-or-not/*

63 *Togo signs MoU to establish MOSIP digital identity system https://www.biometricupdate.com/202011/ppps-and-social-media-influencers-for-biometrics-registration-and-national-id*

64 *Deadline looms for biometric SIM card registration in Tanzania https://advox.globalvoices.org/2020/01/08/deadline-looms-for-biometric-sim-card-registration-in-tanzania/ Togo hopes to launch a new biometric ID in 2021 https://citizenshiprightsafrica.org/togo-hopes-to-launch-new-biometric-id-card-in-2021/;*

65 *Togo https://data.unicef.org/crvs/togo/*

66 *Faure Gnassingbé announces a big bang in the Civil Registry https://www.togofirst.com/fr/gouvernance-economique/1202-4924-faure-gnassingbe-annonce-un-big-bang-dans-letat-civil*

Under the programme, all residents will be registered and will receive a 10-digit unique identification number, which is expected to serve as a basis for public, social and private services delivery. The e-ID will be developed by IIIT-Bangalore using MOSIP (Modular Open-Source Identification Platform).[67]

The country amended its civil registration Law No. 2020-009 of September 10, 2020,[68] on the biometric identification of individuals to, among others, empower the national identification agency (ANID) to collect demographic and biometric data of Togolese citizens as a precursor to setting up the foundational database of the country's digital ID card project.[69] An awareness campaign was undertaken prior to the launch of the project.[70]

In Uganda, the government in 2014 launched mass registration for biometric national identity cards which are issued and maintained by the National Identification and Registration Authority (NIRA).[21] The system was provided by Mühlbauer ID Services GmbH, a German company, for EUR 64 million (USD 63.1 million). Other than the identification register, the Authority is also responsible for the registration of births, deaths, adoptions, and aliens. During registration, fingerprints and photos of applicants are captured digitally.

In August 2022, Uganda announced plans to upgrade its current national identity card which was first rolled out in 2014 to include DNA, fingerprints, palm print and eye scan information from 2024, in order to eliminate crime.[72] The card has so far been issued to 26 million people and its mandatory use is tied to access to a wide variety of services, despite individuals who lack the card being excluded from some services.[73]

In 2013, the Zambian government introduced the National Registration Cards (NRC), a low-tech national ID (NID) that captures certain minimum biographic information and biometric information (right thumbprint). The USD 54.8 million Integrated National Registration Information System (INRIS) replaced the paper-based system introduced in 1965 and would issue biometric-based documents such as national registration cards, birth and death certificates, and facilitate voter registration.[74]

A copy of the application is dispatched to the central office and the original application is retained in the district office. The country is in the process of digitising this NRC data to migrate toward a more advanced electronic ID system with biometric authentication. Over eight million identification data points have already been digitised.[75] The system is expected to be the single source of verification of the status of persons living in Zambia such as citizens, residents or immigrants, and facilitate access to transactions and voter registration.[76] The information collected during enrollment includes biometrics such as photographs for facial recognition, fingerprints, and iris images for persons whose fingerprints are not readable or enrolled.[77]

67 *Togo signs MOU to establish MOSIP digital identity system https://www.biometricupdate.com/202112/togo-signs-mou-to-establish-mosip-digital-identity-system*

68 *A new milestone could soon be reached in Togo's biometric ID project https://www.togofirst.com/en/economic-governance/1603-9611-a-new-milestone-could-soon-be-reached-in-togo-s-biometric-id-project*

69 *Togo amends law on biometric identification to advance digital ID ambitions https://www.biometricupdate.com/202206/togo-amends-law-on-biometric-identification-to-advance-digital-id-ambitions*

70 *Togo readies for biometric ID launch with awareness-raising campaign https://www.biometricupdate.com/202106/togo-readies-for-biometric-id-launch-with-awareness-raising-campaign*

71 *National Identification and Registration Authority https://www.nira.go.ug/*

72 *Uganda's Military Demands Citizen's DNA For Digital Identity Rollout https://www.visiontimes.com/2022/08/12/uganda-dna-biometric-id-social-credit.html; Museveni wants Ugandans' palm prints, DNA details captured 'to eliminate crime' https://www.africanews.com/2018/02/28/museveni-wants-ugandans-palm-prints-dna-details-captured-to-eliminate-crime//*

73 *Uganda's Military Demands Citizen's DNA For Digital Identity Rollout https://www.visiontimes.com/2022/08/12/uganda-dna-biometric-id-social-credit.html*

74 *Biometrics registration for Zambia's new national ID system underway https://www.biometricupdate.com/202203/biometrics-registration-for-zambias-new-national-id-system-underway*

75 *Ibid cross ref 37*

76 *Biometric citizen identification to enhance voter registration and identification in Zambia https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia*

78 *Biometric citizen identification to enhance voter registration and identification in Zambia https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia*

2.2.2 Biometric Voter Registration and Identification Programmes

Over the last few years, several African countries have adopted the use of biometric registration and biometric voter verification systems (BVVS) with the purpose of ensuring voter equality and safeguarding the integrity of the electoral process. Nevertheless, while biometrics have raised expectations for electoral integrity, they do not automatically prevent rigging.[78] The BVVS can still be manipulated since they only help to verify voters and leave the management of the entire election process to the electoral management bodies.

In Angola, the local press reported in 2021 that the Angolan National Electoral Commission (CNE) implemented an electronic system for the registration and identification of those involved in the electoral process to ensure that the entire process was conducted in a standardised and credible manner. This system included the issuing and distribution of identification cards for the various actors involved, such as delegates, international observers, journalists, and electoral policy to allow for greater control and organisation of the entire process. The registration was implemented on a national scale in over 10 provinces for over 14 million voters.[79]

In Cameroon, the Electoral Code instituted the permanent Biometric Voter Card[80] to ensure transparency and credibility in the upcoming presidential elections. The processing of the biometric voter registration data that started in April 2013 has become a continuous process undertaken to update the register of voters on a regular basis. The production of voter cards and polling station electoral rolls was launched after the data processing stage. These final stages of the biometric registration process which were undertaken between July and August 2013, preceded the assignment of voters to polling stations. The biometric personal voter's card carries the names, date and place of birth, parentage, photo, fingerprints, profession, and address of the holder[81].

The biometric system set up for the management of elections in Cameroon comprised 10 regional biometric centres located in the elections management body (ELECAM's) regional delegations and one national election biometrics centre located at the body's head office in Yaoundé. Each of the 360 municipalities in the country had two enrolment kits, to ensure that enrolment was accessible to all voters, regardless of their residence.

In the Central African Republic, to be registered as a voter, one is required to present documents such as the national identity card, passport, birth certificate, a suppletive judgement (mostly for those who have lost their birth certificate), the military booklet or pension booklet, the refugee card or any other document duly issued in lieu of identification document to the enrollment officer.

In the DRC, it was reported that in 2016, Gemalto, the world leader in digital security, had won an international tender to supply the country's National Independent Electoral Commission (CENI) with 22,000 mobile biometric voter enrolment kits to support a comprehensive update of the national voter register.[82] It was anticipated that Gemalto's fully portable Coesys Mobile Enrolment stations would enable 18,000 enrolment centres to rapidly acquire digital photographs, fingerprint and signature records of citizens, and instantly issue personalised voter cards for the 2019 general elections.[83]

Prior to the 2016 developments, the Independent Electoral Commission (IEC) as it was known then had in 2005-2006, had chosen biometric enrolment for the constitution of the first electoral file in the absence of a civil status file. The introduction of biometrics aimed to have a reliable electoral file that guarantees the unique identification of each voter and to establish trust with all partners in the electoral process.

78 *The productive failures of biometric voting in Africa https://democracyinafrica.org/the-productive-failures-of-biometric-voting-in-africa/*

79 *Angola implements technology system of registration and identification of those involved in the electoral processSource: https://peopleid.zetes.com/pt/reference/angola-implementa-plataforma-tecnologica-para-o-registo-e-identificacao-dos-intervenientes*

80 *See article 84 of Cameroon's Law No. 2012/001 of April 19, 2012 on the Electoral Code, https://bit.ly/3ikeDOf*

81 *https://recef.org/wp-content/uploads/Rapport_Biometrie.pdf*

82 *The Democratic Republic of Congo selects Gemalto mobile biometric enrollment solution to support fair elections https://bit.ly/3xU6vve*

83 *Ibid*

The Kenya Integrated Elections Management System (KIEMS) includes an electronic register, biometric voter registration (BVR), electronic voter identification devices (EVID) and a results transmission system (RTS). The election management body, the Independent Electoral and Boundaries Commission (IEBC), piloted the electronic registration of voters in 2009 in 18 constituencies.[84] This was later expanded to all 290 constituencies during the 2013 general election. The biometric voter registration (BVR) method of registration captures a voter's facial image, fingerprints, and biographic information such as name, gender, identity card or passport numbers, and telephone number. During the voter registration for the 2013 election, the IEBC deployed 15,000 BVR kits supplied by OT Morpho Canada Inc in 24,614 registration centres and captured details of 14.4 million voters.[85]

In 2017, IEBC invested USD 36.4 million to upgrade the KIEMS with the purchase of 45,000 all-in-one tablets each costing USD 786 from Idemia, a French company.[86] A total of 19.6 million voters were registered for the 2017 election with 14,523 candidates participating in the election, which cost the country USD 338.4 million.[87] However, there were massive failures and irregularities during the election, leading to the nullification of the presidential election result. For the 2022 election, the number of registered voters increased by 12.8 per cent to 22.1 million voters.[88] The IEBC deployed 55,100 KIEMS kits, some of which were supplied by Smartmatic International Holding B. V. in 46,229 polling stations where 14.3 million Kenyans participated.[89] The electoral body has faced challenges with the integrity of the electronic register, including duplicate voters, access control and in cross-matching data from the BVR and that of the National Registration Bureau to remove deceased persons, and register new voters, which issues were highlighted in an audit conducted by KPMG prior to the election.[90]

In Lesotho, biometric voter registration was first introduced in the 2002 elections, after the Independent Electoral Commission (IEC) awarded an IT Company called Arivia.Kom a Lesotho loti 15.5 million (USD 940,000.00) contract to deliver a packaged IT solution for the elections, including setting up the sites, software provision, and voter registration which constituted capturing of biological data, fingerprints, photographs and signatures onto the database. The system then produces a voter card the owner will use during the voting process.[91]

The uptake of the new system was positive and the IEC reported that 830,000 voters were registered in the initial period while the target was 900,000 people. For all other following elections, unless it is the first time a person is registering as a voter, there was no need for re-registration. It is only for the upcoming 2022 elections which are to take place on October 7, 2022, that the registration process changed. For these elections, only the national Identity card or ePassport which has the ID number is needed to register, and every intending voter has to update their voters' registration information with their ID details.

In Liberia, the country's National Elections Commission (NEC) has announced plans to transition from optical mark recognition for secure voter registration to fingerprint biometrics as it prepares for the 2023 general elections.[92] According to NEC Chairperson Davidetta Browne Lansanah, portable tablets with fingerprint scanners will be used to capture thumbprints for a biometric voter registry. The transition exercise is slated to start on December 15, 2022, and conclude on March 17, 2023.[93]

84 *Biometric Voter Registration https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR)*

85 *Kenya's Biometric Voter Registration: New Solution, New Problems https://issafrica.org/iss-today/kenyas-biometric-voter-registration-new-solution-new-problems*

86 *Inside the flaws of Kenya's electoral biometrics https://www.lemonde.fr/en/le-monde-africa/article/2022/05/27/inside-the-flaws-of-kenya-s-electoral-biometrics_5984834_124.html*

87 *Citizen TV, 'IEBC chairman Chebukati says the commission needs Ksh 40.9 B for elections' (Citizen TV, August 2021), https://www.youtube.com/watch?v=j0ldLOBZ60A*

88 *Election 2022 to feature highest number of registered voters, polling stations in Kenya's history https://www.standardmedia.co.ke/national/article/2001448421/election-2022-to-feature-highest-number-of-registered-voters-polling-stations-in-kenyas-history*

89 *Declaration of results for the election of president of the republic of Kenya at the National Tallying Centre https://www.iebc.or.ke/uploads/resources/QLTlLJx0Vr.pdf*

90 *KICTANet Technology Observer Mission Preliminary Report https://www.kictanet.or.ke/?mdocs-file=46145*

91 *ITWeb, https://www.itweb.co.za/content/nWJadvb8Ze5MbjO1.*

92 *Liberia plans biometric voter registry with enrollment beginning in December https://www.biometricupdate.com/202209/liberia-plans-biometric-voter-registry-with-enrollment-beginning-in-december*

93 *Ibid cross ref 87*

In Nigeria the government adopted the biometric data collection programme for its voters' registration for a Permanent Voter's Card (PVC) as an Automated Fingerprint Identification System in 2011. At the time, the generated register was considered to be the best ever produced by the INEC and was used for the general elections in 2011 and 2015.[94] In preparation for the forthcoming general election in 2023, the Independent National Electoral Commission (INEC) launched a portal where eligible citizens can register for their new PVC, and registered voters can verify their details. After the online registration on the portal, eligible voters still need to schedule an appointment to have their biometric data, which includes facial images and fingerprints, captured at the INEC office or designated centres.

However, the failure to harmonise data collection creates a lot of waste. For instance, in 2015, NGN 120 billion (USD 627 million) was allegedly spent on elections with an estimated USD 200 million spent on biometric voter registration and card issuance. As the federal government seeks to harmonise the biometric data collected by various agencies in the country before 2023, the INEC database is not linked with the National Identification Number (NIN).

In Senegal, by Decree No. 2016-1536 of 29 September 2016, implementing Law No. 2016-09 of 14 March 2016 instituting an ECOWAS biometric identity card, the government instituted the biometric voter card. This decree repealed the provisions of the law of September 2005 instituting the digitised Senegalese national identity card and gives the ECOWAS biometric identity card a value of national identity card and electoral card – the ECOWAS ID card contains a multi-application electronic chip and can be used for other purposes.

The Biometric Voter Card thus included in the ECOWAS biometric identity card has a unique 17-digit number coded according to gender, region, and date of birth. For voters (persons already registered on the electoral roll), it specifies the voter number, region, department, district, municipality, polling station and national identification number (NIN). Senegalese citizens who are between five and 15 years old may apply to obtain an ECOWAS ID card and those who are 15 years and above must obtain an ECOWAS ID card. Its validity is 10 years.[95]

In Sierra Leone, the government initiated its first biometric voter registration and successfully captured the biometric data of 2.7 million voters in 2012. It was estimated that the cost of voter registration was Le 75,333 (USD 10) per voter, and a smart card that the country plans to introduce may cost Le 120,579 (USD 16). The country's various cards are not interoperable, there are no mechanisms to link the identities across the different identity registers, and the data they contain is often inconsistent and has been described as unreliable.[96] Ahead of the 2018 presidential and general elections, the government adopted a biometric voter registration exercise. The process, which was jointly implemented by the National Electoral Commission (NEC) and the National Civil Registration Authority (NCRA), did not, however, include biometric identification of voters on Election Day.

Ahead of the 2023 elections, the government has attempted to introduce amendments to the Public Elections Act which would require citizens to have a National Identification Number (NIN), essentially requiring biometric registration with the NCRA to be eligible to vote. However, this move was widely condemned by activists who worked toward ensuring that the controversial provisions were removed from the final legislation.

In 2015, the Tanzanian government introduced a Biometric Voter Registration System[97] with a private Dutch company, GenKey, working as a subcontractor for South Africa-based Lithotech Exports, contracted to implement the system through which 24 million eligible voters were registered. In 2021, President Samia Suluhu Hassan indicated that the government was weighing the possibility of introducing biometric voting during the 2025 polls as a way of curbing the number of irregularities common with elections in the country.[98] Furthermore, it would enhance voter participation as experience had shown that many busy voters find it difficult to attend in-person voting.

94 *Introducing BiometricTechnology in Elections https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf*

95 *Decree No. 2016-1536 of September 29, 2016 implementing Law No. 2016-09 of March 14, 2016 establishing an ECOWAS biometric identity card http://www.jo.gouv.sn/spip.php?article10986; ECOWAS biometric identity card: the National Assembly passes the law https://senegalservices.sn/actualite/carte-didentite-biometrique-cedeao-lassemblee-nationale-vote-la-loi*

96 *Ibid cross ref 37*

97 *Biometric voter registration kicks off in Tanzania https://www.aa.com.tr/en/politics/biometric-voter-registration-kicks-off-in-tanzania/72446*

98 *Tanzanian president invokes need for biometric voting to curb election irregularities https://www.biometricupdate.com/202108/tanzanian-president-invokes-need-for-biometric-voting-to-curb-election-irregularities*

In Togo, the Independent National Electoral Commission (CENI) began biometric voter registration in 2014 ahead of the 2015 presidential election. The country used mobile enrollment kits to bring newly eligible voters into the system. During the voter registration drive, CENI used its existing database of three million records to check citizen records, as well as to remove all records of deceased and invalid records, including those that had been lost or duplicated. The CENI verifies both demographic data and biometric data, using fingerprint recognition for the latter. After this two-step verification is complete, citizens receive a printed voter card.

Togo's biometric registration and identification of voters system is provided by Belgium-based Zetes Group which was acquired in 2017 by Panasonic to create the national electoral register.[99] The system allows registration, centralisation in a single database, verification of biometric data by Automated Fingerprint Identification System (AFIS), facial recognition, management of disputes and publication of electoral rolls.[100] The system uses both fingerprint and facial biometrics and was first used for biometric voter registration in 2007, and for subsequent exercises in 2010 and 2013.[101] Through the process, data of three million Togolese was collected and processed.

In Uganda, a biometric voter register was first introduced in 2001 with the implementation of the Photographic Voter Registration and Identification Systems (PVRIS) project, becoming one of the first adopters of biometrics in Africa[102]. Voters were registered using a digital camera to capture a photograph of the voter, and biographical data was captured using a paper-based registration form. In 2016, the Electoral Commission adopted the Biometric Voter Verification System (BVVS) with fingerprints and images of all registered voters. These voters' records (which in the 2016 elections related to more than 15.27 million individuals) were sourced from the National Security Information System, which is managed by the National Identification and Registration Authority (NIRA) and is the basis for issuing national IDs. The BVVS uses fingerprints to match voter details to confirm that the person is on the voters' roll for a given polling station. The data in the BVVs includes the name, place and date of birth, location of the polling station and fingerprints of the voter. The BVVS was also used in the 2021 elections, effectively disenfranchising citizens who did not possess national IDs.

In 2020, the Zambian government, with support from the United Nations Development Programme (UNDP), chose Smartmatic International, to implement biometric voter registration as a way of improving the country's voter register.[103] The voter registration project in Zambia is part of the UNDP's ongoing commitment to improving the performance of democratic governments. The system uses fingerprint and facial scanning technology to capture biometric data as well as record copies of identification cards. The system was implemented across the country and captured the data of the seven million persons that voted in the August 2021 general elections.

2.2.3 Government-led CCTV Programmes with Facial Recognition

The launch of mobile-based facial recognition by mobile phone companies such as Apple's FaceID and the various Android-based systems accelerated the uptake and acceptance of fingerprint and face-based authentication systems.[104] The emergence of the COVID-19 pandemic coupled with the rapid development of artificial intelligence in recent years also spurred the deployment of facial recognition technology. Facial recognition has been used for COVID-19 contact tracing in South Korea, China, Russia, India, Russia, Poland and the United States.[105]

99 *About Us, https://peopleid.zetes.com/en/about-us*

100 *ZETES In Charge of Voter Registration for the recent municipal elections in Togo https://peopleid.zetes.com/en/Togo-Local-Elections-2019; Biometric Registration in Togo https://peopleid.zetes.com/en/reference/biometric-voter-registration-togo*

101 *Biometric voter registration in Togo https://peopleid.zetes.com/en/reference/biometric-voter-registration-togo*

102 *Introducing Biometric Technology in Elections https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf*

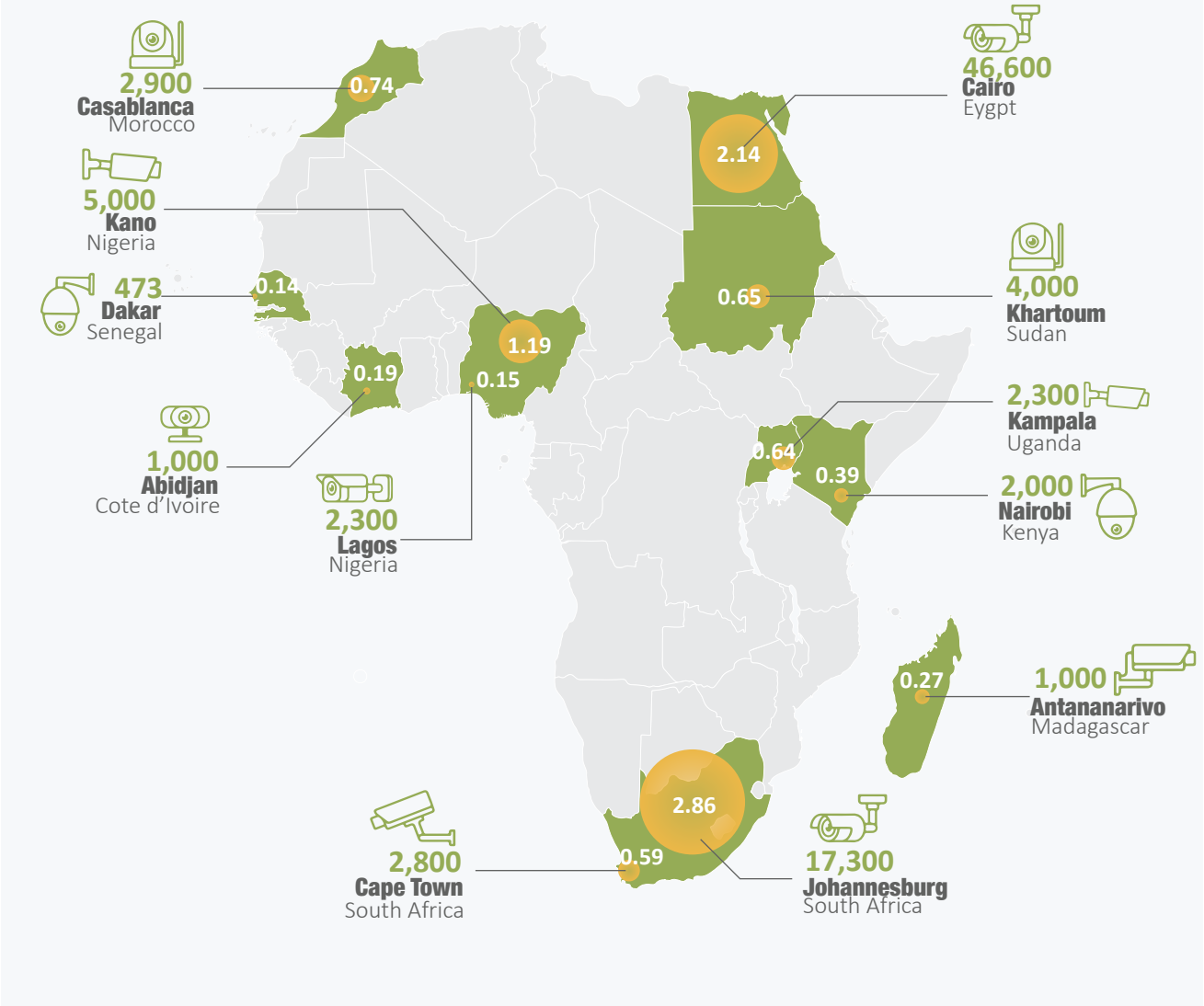
103 *Zambia: Country's voter register goes over to biometrics https://www.smartmatic.com/us/case-studies/article/zambia-countrys-voter-register-goes-over-to-biometrics/*

104 *It's a New Decade for Biometrics. Let's wrap up 2019 and take a look at what's in store for 2020 https://www.acuitymi.com/post/it-s-a-new-decade-for-biometrics-let-s-wrap-up-2019-and-take-a-look-at-what-s-in-store-for-2020*

105 *Keep Facial Recognition Away from COVID-19 Response https://www.cato.org/blog/keep-facial-recognition-away-covid-19-response*

Several countries have deployed closed-circuit television camera (CCTV) surveillance in major towns and streets. Some of these projects have been implemented as part of Huawei's Safe City.[106] The product systems include the establishment of command centres, CCTV cameras, intelligent video surveillance, facial and licence plate recognition technology, crowd monitoring, situational awareness detection, noise monitoring or detection, abandoned object detection, and social media monitoring.[107] As of 2019, the state-owned CCTV systems had been implemented in several countries around the continent, including Algeria, Angola, Botswana, Cameroon, Egypt, Ethiopia, Ghana, Ivory Coast, Kenya, Madagascar, Mauritius, Morocco, Nigeria, South Africa, Tunisia, Uganda, Zambia and Zimbabwe.[108] However, the concerns on such technologies include algorithmic bias, hacking, privacy violations, security concerns, and legal compliance, especially with respect to consent and how data is obtained.[109]

The Figure below shows the estimated number and density of CCTV cameras in select cities in Africa.[110]



106 *Huawei Unveils Safe City Solution Experience Center at 2016 Mobile World Congress https://www.huawei.com/us/news/2016/2/unveils-safe-city-solution-experience-center*

107 *Is Huawei's Safe City safe for African cities? https://techcabal.com/2021/08/04/is-huaweis-safe-city-safe-for-africans/; Watching Huawei's "Safe Cities" https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf*

108 *Huawei's Surveillance Technology Program "Safe Cities" Now Active in 12 African Countries https://chinaglobalsouth.com/2019/11/13/huaweis-surveillance-technology-program-safe-cities-now-active-in-12-african-countries/*

109 *Future of facial recognition technology in Africa https://issafrica.org/iss-today/future-of-facial-recognition-technology-in-africa*

110 *Surveillance camera statistics: which cities have the most CCTV cameras? https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/*

As shown in the table above, some of the African cities with the highest density of CCTV are: Johannesburg, South Africa with 17,300 cameras (2.86 per 1,000 people); Cairo, Egypt with 46,600 cameras (2.14 per 1,000 people); and Kano, Nigeria with 5,000 cameras (1.19 per 1,000 people).

In Angola, the Integrated Center for Public Security (CISP) launched in December 2019 and operated by state security forces uses CCTV cameras to monitor citizens in the country's capital Luanda.[111] There are an estimated 955 cameras in the city installed by Huawei and equipped with facial recognition capability.[112] State security agencies are permitted under Angolan law to install surveillance cameras without prior authorisation, and law enforcement agencies can deploy surveillance technology including spyware and communication interception as needed. [113]

In 2014, Cameroon piloted 70 CCTV cameras in six major cities, and later increased them to 1,500[114] for video surveillance as part of the country's Intelligent City Project using Huawei's Safe Cities system.[115] In 2019, the government launched the National CCTV Command Centre and proposals are being considered to add 7,000 cameras to the ecosystem.[116]

In the meantime, Cameroon's Ministries of Territorial Administration and Posts and Telecommunications are considering the installation of facial recognition through the e-police service offered by the National Emergency Telecommunications Network (RNTU). This network was launched on January 5, 2017, at an estimated cost of over 77 billion CFA francs (USD 120.7 million) and offers services designed to ensure the safety of people and their property in the country's 10 cities. These services include standard and emergency calls, e-police, video surveillance and conferencing. The gendarmerie and the police are already using CCTV cameras for their investigations. The e-police service is based on terminals installed in 50 gendarmerie stations throughout the country. It enables the storage of citizens' information in police databases, as well as tracking of individuals based on their fingerprint or facial recognition.[117]

Kenya was one of the first countries to deploy Huawei's African Safe Cities system, which connected 1,800 high-definition cameras and 200 high-definition traffic surveillance infrastructure across the capital, Nairobi in 2014.[118] The Public Safety Communication and Surveillance System (IPSCSS) project[119] aimed to aid crime prevention and accelerate response and recovery. However, data from the National Police Service indicate the system has not yielded much reduction in crime rates in the city, where crime increased between 2017 and 2018.[120] Further, Kenya's airports have been using facial and fingerprint technology installed in 2019. The Japan-funded Comprehensive Community Stabilisation in the Kenya Coast and Key Border Points project[121] supported the installation of NEC's[122] NeoFace Watch facial recognition technology.[123] The same technology has been deployed across major roads and highways as part of an upgrade to the country's Integrated Command and Control System (ICCS) CCTV network.[124]

111 *All for My Cuba https://tudoparaminhacuba.wordpress.com/2019/12/30/pr-abre-centro-integrado-de-seguranca-publica/*

112 *Surveillance camera statistics: which cities have the most CCTV cameras? https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/*

113 *Freedom of the Net 2020: Angola https://freedomhouse.org/country/angola/freedom-net/2020#footnote6_pib2ugn*

114 *Security: FCFA 22,95 Billion for Expansion of Urban Intelligence Video surveillance Project https://cameroon-report.com/securite/security-fcfa-22-95-billion-for-expansion-of-urban-intelligence-video-surveillance-project/*

115 *Cameroon unveils Huawei-built video surveillance centre https://itweb.africa/content/rW1xL759r3B7Rk6m*

116 *Security or privacy invasion: Huawei instals more CCTV cameras in Cameroon https://techpoint.africa/2019/08/29/huawei-cctv-cameroon*

117 *Technology: Facial recognition soon effective in Cameroon https://www.237online.com/technologie-la-reconnaissance-faciale-bientot-effective-au-cameroun/*

118 *The Spread of Surveillance Technology in Africa Stirs Security Concerns https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/*

119 *Is surveillance a panacea to Kenya's security threats https://giswatch.org/en/country-report/communications-surveillance/kenya#sdfootnote11sym*

120 *The Impact of Chinese Tech Provision on Civil Liberties in Africa https://www.africaportal.org/documents/20819/Policy-Insights-99-gagliardone.pdf*

121 *NEC facial recognition border tech for Kenya as airport biometrics rollouts continue https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue*

122 *NEC www.nec.com*

123 *NeoFace Watch https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html*

124 *Kenyan police launch facial recognition on urban CCTV network https://www.biometricupdate.com/201809/kenyan-police-launch-facial-recognition-on-urban-cctv-network*

In Lesotho, where there are currently no government-led CCTV programmes with facial recognition, there are a few CCTV systems in place, which are run by different government departments, such as the military which conducts video surveillance of some locations. Liberia has no formal government CCTV programme. However, individual and private businesses are at liberty to acquire CCTV cameras with facial recognition and use them at will.

In 2016, the government of Mozambique began the installation of CCTV surveillance in the cities of Maputo and Matola, purportedly for security purposes. The project was allegedly awarded without a public tender.[125] The project would involve the installation of 450 surveillance cameras in Maputo and Matola as part of the National Information Interception Command project, which also included an alleged "phone tapping" plan to snoop on the public.[126]

In Nigeria, the federal government awarded a USD 470 million contract for the installation of 2,000 CCTV cameras in Abuja and Lagos to a Chinese firm, ZTE Communications, in 2010.[127] Two government ministries, namely the Ministry of Finance and the Ministry of Police Affairs, as well as the Nigerian Communications Satellite Limited (NIGCOMSAT), signed a tripartite agreement for the management of the CCTV cameras. The agreement holds the Federal Ministry of Finance as the borrower of the fund, the Ministry of Police Affairs was designated as the beneficiary, and the Nigerian Communication Satellite Limited was listed as the operator. The project was expected to be delivered by July 2011.[128] However, the project was abandoned by the government after CCTV was fixed. Thus, a lot of the CCTV cameras installed in Abuja are not working.[129]

In its quest to implement the Smart City initiative, Lagos State began the installation of 2,000 CCTV cameras. The Commissioner for Science and Technology, Hakeem Popoola Fahm, made the disclosure at the 2021 ministerial press briefing to commemorate the second year in office of Governor Babajide Sanwo-Olu's administration. The Lagos government had earlier installed 100 CCTV in the Ikeja metropolis.[130] Meanwhile, the Lagos State Vehicle Inspection Service uses licence plate recognition of CCTV images to monitor traffic offenders and impose sanctions on erring vehicle owners, with the fine ticket sent to the address and phone number of the owner of the offending vehicle. Some law enforcement agents in Lagos State reportedly now wear body cameras.[131]

In a bid to fight insecurity in Ondo State following the June 2022 attack on a church in which up to 40 individuals were killed, the governor of the state signed an executive order for the compulsory use of CCTV devices in public and private institutions. He stated that the executive order would be enforced in places of worship, financial institutions, educational institutions, and event centres as well as other places regularly used by the public. The executive order also states that the installed CCTV devices, apart from capturing all activities at the public and private institutions, must also have data storage hardware and data stored therein should be made available to security agencies whenever it is required.[132]

125 *Club for Mozambique, 'Citizens to be monitored 24 hours a day – Global Voices, https://clubofmozambique.com/news/mozambique-citizens-to-be-monitored-24-hours-a-day-global-voices/*

126 *Mozambique: Citizens to be monitored 24 hours a day – Global Voices https://clubofmozambique.com/news/mozambique-citizens-to-be-monitored-24-hours-a-day-global-voices/*

127 *Abuja $470m CCTV camera project lies in ruins https://guardian.ng/sunday-magazine/cityfile/abuja-470m-cctv-camera-project-lies-in-ruins/*

128 *https://www.tekedia.com/the-nigerias-cctv-bill/*

129 *https://www.premiumtimesng.com/news/163975-high-level-corruption-rocks-470million-cctv-project-secure-abuja.html*

130 *https://www.sunnewsonline.com/lagos-begins-installation-of-2000-cctv-cameras/*

131 *Surveillance Law in Africa: a review of six countries https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=*

132 *Akeredolu orders compulsory installation of CCTV in public places https://punchng.com/akeredolu-orders-compulsory-installation-of-cctv-in-public-places/*

In June 2021, the Secretary General of the High Authority for Airports in Senegal (HAAS), Colonel Ababacar Sédikh Diouf, announced the planned installation of a video surveillance system with facial recognition. This system would enhance airport and national security and would connect to the Interpol database and the list of wanted terrorists. To date, there is no evidence that this system has been set up at Dakar airport.[133]

In Sierra Leone, there were media reports in 2017 that the Sierra Leone Police (SLP) was investing Le4.5 billion (USD 294,213) in CCTV cameras as part of their Safe City Project. During the 2018 budget hearing on August 21, 2017, the SLP announced they would also be installing the national digital radio communication system, with a 112 Toll-free call line and setting up of the control room which would enable the force to respond to crime, other security threats and public disorder.[134]

In Tanzania, the government embarked on a CCTV installation spree in prisons,[135] Mukumi National Park,[136] as well as round the 25-kilometre Mirerani wall[137] north of the country with the purpose of controlling theft within the prisons, curbing poaching as well as theft of minerals to control theft of tanzanite minerals, respectively. In 2018, the country installed the biometric border screening system with facial recognition at Kilimanjaro and Julius Nyerere International Airports using technology provided by Vision-Box.[138]

In October 2018, Uganda's President Museveni commissioned a CCTV surveillance centre with facial recognition capability supplied by Chinese telecommunications giant Huawei Technologies. The USD 126 million system included the installation of 2,300 cameras covering Metropolitan Kampala.[139] The national CCTV system initially included 83 monitoring centres, manned by 522 operators and 50 commanders. Authorities stated that there were plans to integrate it with other Ugandan agencies such as the Uganda Revenue Authority and the immigration department.[140]

In January 2020, the second phase was rolled out to cover 2,319 municipalities and major towns. In 2022, the Uganda Police Force indicated that they needed 20,000 more cameras to cover the country and a project to install an additional 5,000 cameras to cover Kampala's slums was underway at a cost of USD 50 million.[141] Opposition leaders in the country have in the past opposed the CCTV project as a ploy to track and persecute opposition leaders as opposed to tracking crime.[142]

On its part, the Zambian government in 2020 reportedly deployed surveillance camera project solutions on the roads, ostensibly to help in curbing crimes and enable the police to monitor hot spots in crime-prone areas. Codenamed the Advanced Road Safety Management System and the Intelligent Mobility Solutions (IMS) – Safe City Project, the initiative was implemented by a Chinese company, Zhongxing Telecommunication Equipment (ZTE) Corporation.[143]

133 *Senegal: Blaise Diagne International Airport starts facial recognition https://www.aeronautique.ma/Senegal-L-Aeroport-international-Blaise-Diagne-se-met-a-la-reconnaissance-faciale_a4843.html*

134 *Police to install CCTV cameras across Freetown https://zainabijoaque.wordpress.com/2018/03/16/police-to-install-cctv-cameras-across-freetown/*

135 *Tanzania: Govt Installs Detectors, CCTV Cameras in Prisons https://allafrica.com/stories/202005270227.html*

136 *Tanzania to install cctv cameras in southern sanctuary to curb poaching https://www.savetheelephants.org/about-elephants-2-3-2/elephant-news-post/?detail=tanzania-to-install-cctv-cameras-in-southern-sanctuary-to-curb-poaching*

137 *Tanzania installs CCTV cameras to control theft of minerals https://www.newtimes.co.rw/article/164162/News/tanzania-installs-cctv-cameras-to-control-theft-of-minerals#:~:text=Surveillance%20cameras%2C%20scanners%20as%20well,been%20commissioned%20by%20the%20government.*

138 *Tanzanian Authorities Adopt Vision-Box Tech for Biometric Airport Screening https://findbiometrics.com/tanzanian-authorities-adopt-vision-box-tech-501292/*

139 *Uganda's cash-strapped cops spend $126 million on CCTV from Huawei https://www.reuters.com/article/us-uganda-crime/ugandas-cash-strapped-cops-spend-126-million-on-cctv-from-huawei-idUSKCN1V50RF*

140 *Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/*

141 *Uganda Police asks for 5,000 CCTV cameras to monitor slums https://www.independent.co.ug/police-ask-for-5000-cctv-cameras-to-monitor-slums/*

142 *Uganda invests $126M in CCTV with facial biometrics from Huawei https://www.biometricupdate.com/201908/uganda-invests-126m-in-cctv-with-facial-biometrics-from-huawei*

143 *ZM: Surveillance camera projects deployed to watch on people http://www.ifg.cc/aktuelles/nachrichten/regionen/568-zm-sambia-zambia/58826-zm-surveillance-camera-projects-deployed-to-watch-on-people.html*

2.2.4 Biometric National ePassport Programmes

In July 2016, the African Union (AU) unveiled the continent's first electronic passport, during an AU Summit in Kigali, Rwanda, with the aim of distributing them to all African citizens by 2020 so as to ease movement on the continent.[144] While this has not come to pass, several countries and economic blocs have embraced the concept and introduced electronic passports to their citizens, which have electronic chips to store the biometric information of the passport holder.

The implementation of ePassports requires the deployment of advanced digital border management systems including biometric data collection and processing infrastructure, access control systems, biometric identification databases, public key directories, and information sharing protocols to serve a country's border points. Most of these systems are expected to be interoperable and developed in line with the International Civil Aviation Organisation (ICAO) standards and recommended practices.[145] According to ICAO, more than 140 states and non-state entities such as the United Nations are currently using ePassports, with over 1 billion ePassports in circulation.[146]

In April 2017, the East African Community (EAC) Council of Ministers directed Partner States (Burundi, Democratic Republic of Congo, Kenya, Rwanda, South Sudan, Tanzania, and Uganda) to commence issuance of the new EAC ePassport by January 31, 2018,[147] and phase out the old passports by November 2022.[148]

In the Democratic Republic of Congo (DRC), there were media reports in 2016 that a new biometric passport model that contains an electronic chip had been officially unveiled on November 10, 2015.[149] The passport which is compliant with ICAO standards and the issuance system were developed by Semlex, a Belgian company.[150] The information collected include photographs, fingerprints and other personal information together with a registration fee of USD 185, shared between the government (USD 65 and Semlex (USD 125).[151] In June 2022, it was reported that there was controversy surrounding Semlex contract, including accusations of corruption and money laundering in the DRC[152] and its projects in other African countries such as Côte d'Ivoire and Kenya.[153]

The Kenya government was the first in the EAC to roll -out the ePassport in September 2017 after its announcement in December 2016 to replace the first-generation passport.[154] The initial cost of the project was KES 1.5 billion (USD 12.4 million) and was expected to triple by the third year. Pakistan's National Database and Registration Authority (NADRA) won the tender for the ePassport system and had issued 775,000 passports in May 2019. The passports are compliant with ICAO standards, feature linkage with Public Key Infrastructure (PKI), an RFID Chip, and it is integrated with biometric features such as facial image and fingerprints.[155] The ePassport costs between USD 37.7 and 62.6 depending on the number of pages and USD 99.9 to replace if lost.[156] The deadlines for phasing out the old passport have been extended on several occasions since 2018 to the most recent, November 30, 2022, for all EAC Partner States.[157]

144 *United States of Africa? African Union launches all-Africa passport https://www.cnn.com/2016/07/05/africa/african-union-passport*

145 *ICAO TRIP Guide on Border Control and Management https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf*

146 *ePassport Basics https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx*

147 *EAC to start issuing EA ePassport January 2018 https://www.eac.int/press-releases/148-immigration-and-labour/754-eac-to-start-issuing-ea-ePassport-january-2018*

148 *Kenya Sets Deadline For Migration To EAC E-Passport https://cioafrica.co/kenya-sets-deadline-for-migration-to-eac-e-passport/*

149 *Le Potentiel 13 Nov. 2015; Radio Okapi 10 Nov. 2015; Congo virtuel 10 Nov. 2015*

150 *Democratic Republic of the Congo: Biometric passports with electronic chips issued since November 2015, including the application procedure and requirements, as well as the validity period (2015-July 2016) https://www.refworld.org/docid/57a18bdf4.html*

151 *Democratic Republic of the Congo passport https://en.wikipedia.org/wiki/Democratic_Republic_of_the_Congo_passport*

152 *Congo's troubled, lucrative biometric passport contract still open? https://www.biometricupdate.com/202207/congos-troubled-lucrative-biometric-passport-contract-still-open*

153 *Investigations identify the extent – and limitations – of Semlex's political networks in Africa https://www.biometricupdate.com/202010/investigations-identify-the-extent-and-limitations-of-semlexs-political-networks-in-africa*

154 *Kenya goes it alone on e-passport as neighbours dither https://www.theeastafrican.co.ke/news/Kenya-goes-it-alone-on-e-passport-as-neighbours-dither-/2558-4082904-tndadyz/index.html*

155 *Electronic Passport System Kenya https://www.nadra.gov.pk/international-projects/e-passort-for-kenya/*

156 *Transition from the Old Generation Passports to the New Generation E-Passports in Kenya https://cmadvocates.com/transition-from-the-old-generation-passports-to-the-new-generation-e-passports-in-kenya/*

157 *Shambolic Migration to New Kenyan E-Passport https://www.theelephant.info/features/2022/01/07/shambolic-migration-to-new-kenyan-e-passport/*

Tanzania became the second country in the EAC to adopt the ePassport in a project that commenced in September 2017 and launched in February 2018.[158] The project was financed by the government of Ireland with HID Company supplying the services at a cost of USD 57.82 million.[159] The National ePassport program is implemented by the immigration department and registration commences with an online application where applicants are required to provide their NIDA number. The registration process utilises the person's biometric data collected through NIDA and the immigration department together with documents such as birth certificates, national identity cards, affidavits of birth or certificates of naturalisation.[160] The biometric information collected includes the applicant's fingerprints, photograph and signatures. The ePassport which costs USD 67.5, replaced the old passport which was phased out in January 2020.[161]

Uganda launched the ePassport in 2018 Uganda and in May 2022, became the first EAC Partner State to fully transition to the EAC ePassport following a directive of the EAC urging all States to phase-out old Machine-Readable Passports (MRP).[162] Uganda's ePassport is compliant with ICAO standards and includes an RFID chip, biographic information, and secure biographic information such as fingerprints and facial images. The ePassport is linked to the holder through their National Identification Number (NIN). The documents required during application include national identity cards, birth certificates, letters of consent, and where applicable documents supporting an applicant's profession.[163]

The application for the ePassport in Uganda is done online at a cost of USD 67.81. Notably, the online portal contains an explicit privacy policy which requires the consent of the applicant before proceeding. It provides that the information disclosed will be used for the specific purpose of the service offered, and is kept for a limited period to fulfil the purpose for which it was collected.[164] In addition, it states that the agency commits to take precautions to protect an applicant's information from "any loss or illegal usage, access and disclosure" and that the information is secured by standards with regard to its sensitivity.

In Cameroon, the issuance of the biometric passport is done by the National Passport Production Centre linked to the General Delegation of National Security (DGSN). Applicants must fill out their personal data in an online application form and once this data has been validated and payments made, the completed identity data file is generated for download. The second phase consists of physical registration where the signature, fingerprints and photo are collected after verification of the information provided online.[165]

The Central African Republic has been issuing biometric passports since 2012, in compliance with the Monetary and Economic Union of Central African States (CEMAC) requirements.[166] In Lesotho, the Ministry of Home Affairs through its passport offices introduced electronic passports in 2013. To apply for the ePassport, as described in the Lesotho Passport and Travel Act 2018, one needs to fill out the application form available at the passport offices and submit a copy of the identity documents. If the applicant is under 16 years, then their birth certificate and written consent by parent or guardian are required. During the appointment, a passport-size photo and 10 fingerprints for anyone 16 and older are taken. The fingerprints of minors are not taken.

158 *Biometric Passport for Tighter Immigration and Border Control in Tanzania https://www.m2sys.com/blog/e-governance/biometric-passport-for-tighter-immigration-and-border-control-in-tanzania/*

159 *Tanzania launches e-Passport as Magufuli calls for tighter control of illegal immigrants https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-e-passport-as-magufuli-calls-for-tighter-control-of-illegal-immigrants-2621606#:~:text=President%20John%20Magufuli%20has%20on,key%20role%20in%20revenue%20collection*

160 *Passports and Travel Documents Information https://www.immigration.go.tz/index.php/immigration-services/passports-and-travel-documents*

161 *Tanzania introduces electronic passports https://www.africanews.com/2018/02/01/tanzania-introduces-electronic-passports//*

162 *Uganda leads East Africa in fully switching to e-passport https://www.theeastafrican.co.ke/tea/news/east-africa/uganda-leads-east-africa-in-switching-to-e-passport-3825742*

163 *Ordinary Passport https://www.immigration.go.ug/passports/ordinary-passport*

164 *Disclaimer https://www.passports.go.ug/*

165 *A biometric passport in 48 hours in Cameroon https://www.crtv.cm/2021/06/un-passeport-biometrique-en-48h-au-cameroun/; Cameroon Police https://www.dgsn.cm/; Welcome to the Cameroon electronic passport pre-enrollment portal https://portal.passcam.cm/*

166 *Ibid cross ref 11*

The Liberia Passport Office under the Ministry of Foreign Affairs is authorised to issue Passports. The Ministry provides applicants with online and in-person passport application services. As part of the application process, citizens' biometric information including photographs and fingerprints is taken. According to the Ministry, the new Liberian ePassport booklet comes with advanced technology, which no longer has a 2D bar-code, but rather a Radio-frequency identification (RFID) microprocessor chip implanted in the booklet without the ability of detection by touch. The new Liberian Biometric ePassport is compliant with ICAO standards

In Nigeria, the ePassport by the Nigeria Immigration Service (NIS) has been fully harmonised and integrated with NIMC following the provision of mandatory linking of NIN with the ePassport. The NIS introduced the ePassport on May 17, 2007. The use of the ePassport has become a major tool in the fight against trans-border crime as it contains biometric data such as fingerprints and facial images as well as digital signatures of holders.

In 2019, NIS implemented a new requirement for foreign nationals staying in Nigeria for more than 90 days to visit the NIS office to get their biometrics data captured, as well as submit other personal information to be registered before December 31 of the same year. Immigrants who entered the country after December 31, 2019, and sought to remain in Nigeria for over 90 days are required to register under the system.

The Senegalese state introduced the biometric passport with a chip in October 2016 under the Directorate of the Police of Foreigners and Travel Documents (DPETV) of the Ministry of the Interior that collects, processes, and prints the passports. However, the implementation and maintenance of the issuing system is carried out by IRIS Corporation Berhad, a Malaysian company.

In Sierra Leone, applicants for passports are required to appear at the immigration offices where their biometrics (fingerprints) are captured. They are also required to submit or have their passport-size photographs taken.[167]

In Togo, the biographical data collected on a physical form are entered at the bottom and then the applicant gives access to his biometric data such as fingerprints of all fingers, as well as their photo and signature.

Zambia does not issue ePassports to its citizens. However, biographic information together with photographs and fingerprints are collected during the passport application process. Further, documents such as birth or adoption certificates, national registration cards (NRC), marriage certificates, and affidavits are also collected.[168] The ordinary passport costs between USD 80 and USD 100 depending on the number of pages.[169]

2.2.5 Biometric Data Processing Programmes used in Refugee Registration

To improve their service delivery, several humanitarian organisations working with refugee and migrant communities such as the United Nations High Commission for Refugees (UNHCR) have embraced digital technologies such as biometrics, spatial mapping, and social media platforms in humanitarian programming.[170] This technology became even more relevant when the UN Sustainable Development Goal 16.9 gave every person the right to a legal identity, including birth registration, by 2030.[171] Biometric data captured during refugee registration by the UNHCR in its 78 operations globally include fingerprints, facial features, and iris scans for all persons above the age of five in addition to other information in identity documents.[172]

167 *Documentary evidence for ordinary passports https://slid.gov.sl/ordinary-passport/*

168 *Application requirements for a Zambian Passport or Travel document of Identity http://zambiahighcommission.ca/wp/wp-content/uploads/app_passport_guide.pdf*

169 *Passport application https://www.zambiaembassy.org/page/passport-application*

170 *ANALYSIS: Digital humanitarianism in Africa: hope or hype? https://www.premiumtimesng.com/news/headlines/551771-analysis-digital-humanitarianism-in-africa-hope-or-hype.html*

171 *Ibid*

172 *Biometrics, UNHCR https://help.unhcr.org/jordan/wp-content/uploads/sites/46/2022/04/Biometrics-EN_Final_April2022.pdf*

In Cameroon, the collection of biometric identification of refugees has been taking place since 2016 under UNHCR leadership. It involves all 1.7 million[173] refugees under the mandate of the UNHCR in Cameroon and enables the agency "to have updated data likely to facilitate refugees' access to humanitarian assistance and ensure their protection", according to the UNHCR spokesperson. The refugees are required to register their fingerprints, photographs and iris scans.

This is a continuous operation which aims to update basic identity data, enrol refugees who are more than four years old, carry out in-depth identification of people with special needs, and collect data on intentions to return and renew all documents (allocation cards and refugee attestation).[174] In 2022, authorities launched a pilot biometric project to issue 6,000 biometric-based identity cards to refugees from the Central African Republic based in the Eastern region of the country, which will be scaled to cover the remaining 300,000 refugees in the country.[175] The project is implemented in partnership with the UNHCR and financed by the World Bank with technical support from Impact Palmarès R&D.

In the DRC, the UNHCR is the main agency working in the refugee sector in collaboration with the DRC national commission for refugees. The UN agency is understood to have a data management department that collaborates with the Protection Unit on biometric data collection.[176] The country has 498,959 refugees, 5.6 million internally displaced persons (IDPs), and 1.6 million returned IDPs.[177]

According to the UNHCR, Kenya had a total population of 504,932 persons comprising refugees (81%), asylum-seekers (14%) and stateless persons (3%) in 2022, a majority of whom are from Somalia (259,040), South Sudan (118,655) and Democratic Republic of Congo (48,968).[178] Persons seeking refugee or asylum status are required to register with the Government of Kenya Refugee Affairs Secretariat.[179] The registration is done in Kakuma and Nairobi and employs a unified data management system which is combined with a biometric system. After the registration, a refugee identification card, refugee certificate or alien card is issued.[180]

During registration, the biodata and other important information relating to the applicant, their family and relatives living in Kenya and abroad are collected.[181] Further, passport pictures, fingerprints and iris scans of the applicant and their family members present are taken. Applicants are also required to present documents such as passports, national identity cards, driver's licences, military identity cards, marriage or divorce certificates, family booklets, education certificates, medical records, and proof of previous registration as refugees or asylum in other countries. Once registered, the applicants are provided with proof of registration, asylum seekers pass, a movement pass, and finally a refugee identification card is issued to those who qualify.

173 *Cameroon https://reporting.unhcr.org/cameroon*

174 *Cameroon: Biometric identification of Douala refugees launched by UNHCR https://www.digitalbusiness.africa/cameroun-lidentification-biometrique-des-refugies-de-douala-lancee-par-lunhcr/; Cameroon: Far North Minawao biometric results - April 2018 https://reliefweb.int/report/cameroon/cameroun-extr-me-nord-r-sultats-biom-trie-minawao-avril-2018*

175 *Cameroon begins pilot to issue 6k biometric ID cards to CAR refugees https://www.biometricupdate.com/202207/cameroon-begins-pilot-to-issue-6k-biometric-id-cards-to-car-refugees*

176 *Registration and profiling https://reporting.unhcr.org/node/12365; DR Congo https://reporting.unhcr.org/sites/default/files/UNHCR%20DRC%20Fact%20Sheet%20-%20July%202020.pdf*

177 *DRC https://reporting.unhcr.org/drc*

178 *Kenya https://reporting.unhcr.org/kenya*

179 *Registration and Documentation https://www.unhcr.org/ke/registration*

180 *Recognising Nairobi's Refugees https://www.nrc.no/globalassets/pdf/reports/refugees-in-nairobi/recognising-nairobis-refugees.pdf*

181 *How do I register my application for asylum? https://help.unhcr.org/kenya/applying-for-asylum-in-kenya/how-do-i-register-my-application-for-asylum/*

For refugee registration, Lesotho uses the UNHCR system known as Population Registration and Identity Management Ecosystem (PRIMES). The system was introduced in Lesotho in 2018 and consists of refugee registration, case management as well as Biometric Identity Management System (BIMS) which is the module that collects and manages the biometric data of refugees. This system is cloud-based and managed by UNHCR.[182]

The 2.7 million refugees[183] in Nigeria are required to register for a National Identification Number to aid proper documentation and service delivery to them. In 2021, Nigerian banks and financial institutions began to recognise refugee identity cards issued by National Commission for Refugees, Migrants and Internally Displaced Persons (NCFRMI) and UNHCR, and Convention Travel Document (CTD) provided by the Commission and Nigerian Immigration Service (NIS) to facilitate their identification, banking operations and financial inclusion. Internally Displaced Persons (IDPs) are also required to register for a NIN for proper social integration.

In 2017, the government of Tanzania through the Ministry of Home Affairs, the Immigration Department and the International Organisation for Migration (IOM), are reported to have launched a biometric registration system for irregular migrants in the country's Tanga region.[184] According to the reports, the electronic registration (e-registration) of irregular and settled migrants in Tanzania followed a successful pilot project in the Kigoma region in which more than 22,800 migrants were registered and provided with a personalised laminated photo ID card, which allows them to remain in Tanzania for up to two years, while their immigration status is determined by the Tanzanian authorities.[185] The country has a population of 247,033 refugees.[186]

In 2018, the Ugandan government with support from the UNHCR, launched a large-scale programme to verify the identities of all 1.5 million refugees in the country, using biometric data.[187] The government was reported to be using the UNHCR's biometric registration Population Registration and Identity Management EcoSystem (PRIMES), which is used to register millions of refugees worldwide.[188]

2.2.6 Biometric SIM Card Registration Programmes

Over the last few years, several African countries have sought to link SIM card registration with users' biometrics as captured in the national ID programmes, raising concerns about privacy and data protection as well as the exclusion of categories of people who may not have a national ID. In fact, mandatory SIM-card registration has driven the demand and adoption of digital ID credentials, both of which are critical to access digital services.[189]

In Cameroon, biometric SIM card registration backed by the biometric national identity card has been in force since 2016. Article 6 of the Decree No. 2015/3759 on the identification of subscribers requires SIM card subscribers to provide their original national identity card, their exact address including a location map, and the international mobile equipment identity number (IMEI) of their device. This is in line with article 55 of the eCommunications Act.

In 2019, the Cameroon Telecommunications Regulatory Board (ART) sanctioned mobile operators Orange, MTN and Nextel with fines totalling CFA 3.5 billion (USD 5.9 million) for failure to comply with SIM card registration rules. The telecoms regulator accused the operators of continuing to sell unregistered SIM cards and other failures in properly handling the SIM registration procedures stipulated by the law.

182 *From proGres to PRIMES https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-03-16-PRIMES-Flyer.pdf*

183 *Nigeria https://reporting.unhcr.org/nigeria*

184 *Tanzania Launches Biometric Registration System for Migrants https://www.iom.int/news/tanzania-launches-biometric-registration-system-migrants*

185 *Ibid*

186 *Tanzania https://reporting.unhcr.org/tanzania*

187 *Uganda launches major refugee verification operation https://www.unhcr.org/en-us/news/latest/2018/3/5a9959444/uganda-launches-major-refugee-verification-operation.html*

188 *Ibid*

189 *On the Road to Digital-ID Success in Africa: Leveraging Global Trends https://institute.global/policy/road-digital-id-success-africa-leveraging-global-trends*

The Kenya Information and Communication (Registration of SIM cards) Regulations 2015,[190] require all SIM card subscribers to provide their biographical information such as names, dates of birth, gender, physical address, postal address, other numbers owned, copies of national identity cards, military identity cards, passports or birth certificates to the telecom operator.

In April 2022, Safaricom, Kenya's largest telco was sued for requiring photos of its subscribers, in contravention of the Kenya Information and Communication (Registration of SIM cards) Regulations 2015, and section 31 of the Data Protection Act, 2019.[191] The company stated that the collection of subscribers' photos was aimed at enhancing security and reducing identity fraud in the use of its services.[192] The regulator later clarified to owners of the country's 64.9 million SIM cards[193] that the submission of photos was not mandatory.[194]

In early 2022, Kenya's telecom regulator, the Communications Authority imposed a deadline of April 15 for mandatory SIM-card registration, after which all unregistered SIM cards would be deactivated. However, the deadline for updating subscriber registration details was later extended to October 15, 2022, after public uproar regarding the short timelines to comply with the directive.[195]

The Lesotho Communications Authority (LCA) issued The Communications (Subscriber Identity Module and Mobile Device Registration) Regulations in May 2021. It is mandatory for every SIM card and mobile device utilising telecommunications services within Lesotho to be registered. The registration is done by the telecom companies, and then the database is periodically transferred to the LCA, which is the custodian for the central database as provided for by sections 5(1)-(2) of the Regulations.

Under section 21(1) of the Regulations, diplomats are exempted from having their fingerprints or biometric information was taken. Only passport and diplomatic identity documents are required for them to register their SIM cards. In Lesotho, the process of SIM card registration commenced on June 24, 2022.[196] Although the Regulations do not mention photos as a requirement for the registration process, during registration, face photos are taken.

The government of Liberia, through the Liberia Telecommunication Authority, has imposed mandatory registration of prepaid SIM card users who are required to present a valid ID, passport, and photo or register their biometrics prior to SIM card activation. Existing users who are unable to register their SIM cards within certain periods are blocked or disconnected from various GSM networks.

Following food riots that took place in Maputo in 2010 which were mainly coordinated via SMS, the government decided to introduce SIM card registration. Initially, mobile operators were given a deadline of three months to complete the registration process, which was later extended to 2011. As of 2012, only about half of the SIM cards in use had been registered. In 2015 the government set a new deadline and finally in 2016 a million lines were deactivated for not being registered. Subscribers must produce a passport or national ID to register a SIM card.[197]

In December 2020, Nigeria's federal government directed all citizens and persons legally residing in Nigeria to link their National Identification Numbers (NINs) to their SIM cards, with a threat to disconnect unlinked SIM cards. In 2011, the Nigerian Communication Commission (NCC) budgeted 6.1 billion naira (USD 141.6 million) to conduct biometric registration of SIM cards in the six geopolitical zones of the country in addition to Lagos. The regulator requires telecommunication operators to register the SIM cards of their subscribers in a bid to curb insecurity and crimes. The NCC officially announced that the registration of old SIM cards concluded on June 30, 2013.

190 *Kenya Information and Communication (Registration of SIM cards) Regulations 2015, https://www.ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf*

191 *LSK wants Safaricom compelled to delete subscribers photos https://www.the-star.co.ke/news/2022-04-19-lsk-wants-safaricom-compelled-to-delete-subscribers-photos/*

192 *Sim card registration: Why Safaricom is taking your photos https://www.youtube.com/watch?v=B0zN1ooUKVA*

193 *Third Quarter Sector Statistics Report for the Financial Year 2021/2022 (1st January - 31 March 2022) https://www.ca.go.ke/wp-content/uploads/2022/06/Sector-Statistics-Report-Q3-2021-2022.pdf*

194 *You are not required to submit your photo during SIM card registration – Chiloba https://www.pd.co.ke/news/you-are-not-required-to-submit-your-photo-during-sim-card-registration-chiloba-122677/*

195 *Authority Extends SIM Card Registration Validation Exercise By Six Months https://www.ca.go.ke/authority-extends-sim-card-registration-validation-exercise-by-six-months/*

196 *SIM Registration resumes in June https://www.gov.ls/sim-registration-resumes-in-june/*

197 *Mozambique https://prepaid-data-sim-card.fandom.com/wiki/Mozambique*

As of April 4, 2022, the NCC announced that over 125 million SIM card owners had submitted their NINs for them to be linked, verified and authenticated. The NCC stated that calls by subscribers who had not complied with the NIN-SIM linkage directive would be barred. Part 2 of the Nigerian Communications Commission (Registration of Service Telephone Subscribers) Regulations 2011 establishes the obligation to maintain and operate a central database domiciled within the NCC for the central processing and storage of subscribers' information. Also, regulation 8 provides access to subscriber information on the central database by security agencies. However, it requires that a prior written request specifying the purpose of the request should be made to the NCC from "an official of the requesting security agency who is not below the rank of an Assistant Commissioner of Police or a corresponding rank in any other security agency."

In August 2007, Senegal introduced Decree 2007-937 of 7 August 2007, which requires operators of public telecommunications networks to register all SIM card buyers and users. In 2013, under the pretext of fighting crime linked to the use of mobile telephones, the Senegalese Telecommunications and Postal Regulatory Authority (ARTP) relaunched the SIM card registration exercise. Information required for registration includes a family name, first name, and CNI (ID) number. The SIM card registration data is linked to the national identity database.[198]

Section 3 of Sierra Leone's Telecommunications Subscribers Identification and Registration Management Regulations 2020 requires licensed communications service providers to obtain, record and store information of subscribers.[199] The required customer registration data includes a passport-sized photograph, clearly depicting the facial image of the customer and or biometric information or a copy of a valid identification document. The regulations define biometric information to mean the "fingerprints and facial image" of a subscriber. Other registration data required in accordance with the registration specifications provided by the regulator include the names, date of birth and sex of subscribers.

In Tanzania, SIM card registration is done biometrically by telecom companies that require individuals to have a NIDA-issued identity card or NIN. Per the Electronic and Postal Communications (SIM card Registration) Regulation, 2020, all SIM cards must be registered biometrically or be disconnected. Telecom companies are linked with the NIDA database and they can access the data of the individuals to an extent not disclosed to the public. For SIM card registration, telecom companies collect individuals' fingerprints and digital signatures, while accessing their other personal information through the NIDA database. Tanzania first mandated SIM card registration through the Electronic and Postal Communication Act, 2010 (EPOCA), section 93 of which provides that "Every person who owns or intends to use a detachable SIM card or built-in SIM card mobile telephone shall be obliged to register a SIM card or built-in SIM card mobile telephone".

The registration of SIM cards was made mandatory in Uganda in 2012 following a campaign by the communications regulator, arguing that the exercise was necessary to curb crime by enabling the tracking of criminals and identification of SIM card owners.[200] Subscribers are required to present their national ID to register their SIM cards. In addition, telecom operators have access to an Application Programming Interface (API) provided by the National Identity Registration Authority (NIRA) to verify and validate SIM card registration information. The identity card is verified through a two-stage authentication process through an electronic biometric card reader, and the submission of biographic information to NIRA and a clear photograph.

The Operator must verify the particulars of the national ID card using an Electronic Biometric Card Reader, match the applicant's live biometrics with the biometrics on the card, and obtain real-time verification with the NIRA database through the API.

198 *Decree 2007-937 of 7 August 2007 http://www.osiris.sn///IMG/pdf/document_Decret_relatif_a_lidentification_des_abonnes_153.pdf*

199 *Telecommunications Subscribers Identification and Registration Management Regulations 2020 https://www.natcom.gov.sl/wp-content/uploads/2021/02/The-Telecommunications-Subscribers-Identification-and-Registration-Management-Regulations-2020.pdf*

200 *Mapping and Analysis of Privacy Laws in Africa, https://cipesa.org/?wpfb_dl=479*

2.2.7 Biometrics processing by foreign missions

Many foreign missions based in the countries under review also collect personal data of persons seeking to travel to their countries. The main types of information collected electronically by the US,[201] Canada,[202] European Union[203] and the UK[204] include biographic data (name, date of birth, nationality, place of birth and other personal details on the biographic data page of the applicant's passport), fingerprints, palm prints, handwriting or signatures, and facial images.

2.3 Collection and Processing of minors' biometric data

The main areas where data of minors was collected were in relation to civil registration, including the issuance of birth certificates, national identity cards, ePassports, immigration, health services and SIM card registration. In CEMAC jurisdictions persons above the age of 16 may be issued with a driver's license for Category A or A1.[205] Zambia's digital national identity card will be issued to persons above the age of 16.[206] Kenya's Huduma Namba digital identity card captures the biometric data of children above the age of six.[207] In most countries, SIM cards used by minors are registered either in their names such as in Tanzania, or of their parents or guardians in other jurisdictions.

Foreign missions such as Belgium collect biometrics of children above the age of 12 years.[208] According to VFS Global, Schengen and UK visa applicants are only exempted from the collection of fingerprints if they are under five years of age, although their digital photographs are taken.[209] Further, children under the age of 14 years who are applicants for US and Canadian visas are exempt from the requirement of providing biometric data.[210] Not all countries have such explicit provisions in their laws, policies or practices designed to protect the privacy of children, especially from the collection of their biometric data.

2.4 Justifications for Biometric Data Processing

In introducing several biometric data collection programmes, countries have put forward various justifications including promoting national security, stability, efficient identity information management. Other reasons given include enhancing a country's digital transformation efforts, eliminating identity theft and fraud and counterfeiting of official documents, enhancing tax collection, facilitating movement and border control, fighting corruption and improving service delivery.

In Cameroon, the goal was to develop a centralised population database, enhance transparency, ensure national security, reliable identification and border management, combat counterfeiting of documents, address irregularities in the paper-based systems, and ensure alignment with international standards for ePassports.[211] In the Central African Republic, the collection of fingerprints during voter registration was aimed at enhancing security, eliminating electoral fraud, and improving identification. During the introduction of the biometric passport, it was stated that it would ensure compliance with international standards.

201 *Safety & Security of U.S. Borders: Biometrics https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/border-biometrics.html#:~:text=For%20U.S.%20Visas%20the%20chosen,officer's%20interview%20with%20the%20applicant.*

202 *What biometrics are collected and who must provide biometrics https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/identity-management/biometrics/what.html*

203 *What happens at the Visa Application Centre https://visa.vfsglobal.com/sau/en/che/attend-centre/what-happens-at-centre*

204 *Biometric Enrolment: Policy guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091802/Biometric_information_-_enrolment.pdf*

205 *Regulation No. 04/01-UEAC-089-CM-06 http://www.droit-afrique.com/upload/doc/cemac/CEMAC-Reglement-2001-04-Code-de-la-route.pdf*

206 *Zambia implements biometric ID registration system https://itweb.africa/content/nWJadMbeW5r7bjO1*

207 *Six-year-olds to get IDs in Huduma plan https://nation.africa/kenya/news/six-year-olds-to-get-ids-in-huduma-plan-2303574*

208 *Biometrics https://www.cev-kin.eu/en/general-information/biometrics*

209 *What happens at the Visa Application Centre https://visa.vfsglobal.com/jor/en/cze/attend-centre/what-happens-at-centre*

210 *Safety & Security of U.S. Borders: Biometrics https://travel.state.gov/content/travel/en/us-visas/other-visa-categories/safety.html; Photos and Fingerprints https://www.ustraveldocs.com/ci/ci-niv-photoinfo.asp#:~:text=There%20are%20some%20applicants%20whose,over%20the%20age%20of%2079; What biometrics are collected and who must provide biometrics https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/identity-management/biometrics/what.html*

211 *10 Questions to understand the biometric redesign of electoral rolls in Cameroon https://www.camerlex.com/10-questions-pour-comprendre-la-refonte-biometrique-des-listes-electorales-au-cameroun-12559/*

In the Democratic Republic of Congo, the installation of public CCTV cameras in Kinshasa in 2016 was aimed at enhancing the security of the city and promoting road discipline. The ePassport was also promoted as being part of the State's efforts to comply with international standards and requirements within the EAC and to increase efficiency. Biometric identity cards and SIM card registration are purportedly aimed at fighting crime, reducing identity theft, and improving identification.

In Kenya, the introduction of the Huduma Namba was geared toward having a central database "single source of truth" about the identity of all residents, improving service delivery, improving identification of individuals and verification of identity by state and non-state actors, and curbing fraud and crime. Further, it aimed to reduce the cost of the population census, widen the tax base, improve voter registration, facilitate the issuance of drivers' licences, and eliminate duplicate identity documents required to access government services.[212] The ePassport was adopted as part of compliance with the EAC directive and to upgrade the older generation passport, enhance efficiency at border points, improve the security of the document and prevent its duplication.

In Lesotho, the key reasons given are to curb identity theft, aid the investigation and prevention of cybercrimes, and promote service delivery through a single identity document. In Liberia, the digital identity programme is being implemented to improve human resource management within government, lower the cost of election registration and the census, improve border control and electoral management, access to financial services, reliability of travel documents, tax collection, access to social safety nets and universal health care, harmonise identity programmes across government agencies and within the ECOWAS region.

In Mozambique, identity programmes have been promoted to enhance public order and security, establish an information database, facilitate public services, and improve communications. In Nigeria, the key justifications include promoting national security by combating insecurity and reducing crime; creating a national identity database of the population; improving the identification of residents with accurate data; ensuring strategic national planning; and improving service delivery and tax collection.

In Liberia, increased investment in technology is expected to address corruption in public administration and the judiciary.[213] Further, the digital ID is expected to ease challenges in accessing financial and insurance services and reporting corruption. As Senegal, the biometric national ID card, driver's license, and voter's cards are geared toward preventing identity theft and electoral fraud; promoting access to services; reducing road accident; complying with regional ECOWAS standards and directives; and enhancing efficiency by eliminating duplication of records.[214] The proposed CCTV system aims to improve national security.

For Sierra Leone, the introduction of the multi-purpose National and ECOWAS Identification Cards was expected to facilitate personal transactions, movements, and identification of people.[215] It was also expected to tackle mobile fraud, improve service delivery, fight crime through better information, and reduce the cost of duplicitous data collection processes for elections and civil registration.

In Tanzania, the justifications for the introduction of biometric identification include modernisation of processes and records management from paper-based to digital systems; enhancing national security and preventing crime; improving social welfare; boosting economic development; improving access to social services; providing accurate data of residents; enhancing the efficiency of service delivery, and improving identification of residents through the issuance of documentation.

212 *Benefits https://www.hudumanamba.go.ke/benefits/*

213 *Increased Investment in Technology Can Reduce Corruption in Liberia https://frontpageafricaonline.com/news/tech/increased-investment-in-technology-can-reduce-corruption-in-liberia/*

214 *The advantages of the ECOWAS biometric identity card shared in Kaolack http://www.osiris.sn/Les-avantages-de-la-carte-d.html*

215 *Confirmation and registration of citizens and non-citizens in Sierra Leone to commence soon https://www.thesierraleonetelegraph.com/confirmation-and-registration-of-citizens-and-non-citizens-in-sierra-leone-to-commence-soon/*

The introduction of Togo's e-ID programme was part of the government's promise to digitise public services, have a central database of accurate information on the population, ease administrative processes, facilitate information sharing among agencies and enhance future planning.[216] In doing so, it is expected to facilitate access to credit, enhance access to health services, prevent crime by having information to identify criminals, reduce fraud in the banking sector, ensure the targeted distribution of social and public services, and improve educational and administrative follow-up for citizens.[217]

In Tunisia, the main justifications for introducing CCTV surveillance were to promote national security and fight terrorism. The ePassports and national biometric cards were deployed as part of compliance with international standards to ensure the security, integrity, and interoperability of travel documents. Also, the biometric programmes have been noted as part of modernisation efforts to digitise administrative services to improve service delivery, improve the identification of residents and facilitate information sharing.

The launch of Uganda's ePassport was expected to be instrumental in reducing fraud, document forgery, and identity theft by enhancing the privacy of the holder's information.[218] The document was also expected to ease the handling of entry and exits at all border points and enhance the integrity of the country's passport worldwide. Other justifications for the introduction of biometric systems include the promotion of national security and fighting crimes such as fraud, enhancing the efficiency of registration and accuracy in the identification of residents, promoting of economic and technological development, improving service delivery and access to government services, preventing election fraud, reducing the cost of registration, facilitating national planning, combating corruption, and improving records management.

During the launch of the country's ePassport, Tanzania's former President John Pombe Magufuli (RIP) hailed the project as critical in enhancing national security, controlling illegal immigrants, enhancing revenue collection, improving productivity, and simplifying service delivery.[219] In Zambia, the introduction of the biometric digital identity card is expected to address the challenges of the decades-old paper-based system such as duplication of identity cards, identity fraud, difficulties in the Know-Your-Customer (KYC) operations, and loss of revenue for state and non-state actors.[220] In addition, the system is expected to improve service delivery; reduce electoral fraud; eliminate ghost workers; and enhance the national security of the country, identification of residents, and KYC operations. Further, the system is expected to lead to savings in social cash transfer programmes and to enhance compliance in domestic tax collection and health insurance, while also increasing annual revenue from authentication and verification fees from financial institutions and mobile network operators by up to USD 410 million.[221]

216 *Togo is About to Initiate Biometric ID for All Its Residents https://www.m2sys.com/blog/e-governance/togo-initiate-biometric-id/*

217 *Togo hopes to launch new biometric ID card in 2021 https://www.biometricupdate.com/202012/togo-hopes-to-launch-new-biometric-id-card-in-2021*

218 *How E-Passport Will Ease Travel For Ugandans https://caa.go.ug/how-e-passport-will-ease-travel-for-ugandans/*

219 *Tanzania launches e-Passport as Magufuli calls for tighter control of illegal immigrants https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-e-passport-as-magufuli-calls-for-tighter-control-of-illegal-immigrants-2621606#:~:text=President%20John%20Magufuli%20has%20on,key%20role%20in%20revenue%20collection.*

220 *Biometric citizen identification to enhance voter registration and identification in Zambia https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia*

221 *Ibid; Government Begins implementation of the Biometric Enabled National Registration Cards https://www.lusakatimes.com/2022/03/15/government-begins-implementation-of-the-biometric-enabled-national-registration-cards/; Mutati highlights need for electronic IDs https://diggers.news/local/2022/02/25/mutati-highlights-need-for-electronic-ids/*

3.0 Discussion: Trends, Potential Risks, Challenges and Gaps

3.1 Limited Public Engagement or Awareness Campaigns

While biometric data collection has an overbearing impact on privacy, in many countries there has been a distinct lack of public awareness, engagement and consultations among key stakeholders and the wider public on the purposes, uses, design, and implementation of biometric data collection programmes. In countries where public campaigns were undertaken, data protection principles, data subjects' rights, and potentials for data abuse, were rarely emphasised despite the low levels of privacy awareness among data subjects. Governments all around appear to have been in a rush to launch biometric data collection programmes and to celebrate registration numbers rather than prioritising public consultations and engagement which are critical to the success of such projects.

It was also established that in many countries studied such as Angola, Liberia, Nigeria Mozambique, Tanzania and Zambia, there was minimal or limited public engagement on issues of personal data collection programmes and their intentions and any attendant risks. As a result, and given the power asymmetry between states and data subjects, the public provides biometric data without question or prior informed consent, but out of necessity in order to acquire critical services or official documents such as passports, national identity cards, voters cards or driver's licenses.

Where there have been public campaigns, these have been carried out over short periods and sporadically, often with limited disclosures and misleading information on the technologies and the purpose of the programmes, coercive directives to ensure compliance without question, and mandatory in nature without provision of alternatives to registration and enlisting. For example, in Cameroon, public campaigns by Elections Cameroon (ELECAM) and the National Youth Observatory focused on encouraging people to enrol biometrically for elections and the Biometric Youth Card respectively. Similarly, in Kenya, public campaigns conducted by the Ministry of Interior and the Independent Electoral and Boundaries Commission (IEBC) focused on coercing people to enrol for the Huduma Namba by May 25, 2019,[222] and to register as voters by May 4, 2022.[223] In Uganda, public campaigns prior to the introduction of the national identity card focused on enrollment without similar engagement on the merits of the biometric identity card.

In Senegal, a public campaign held from November 9 to 21, 2019 by the General Directorate of Elections in Senegal (DGE) focused on encouraging and mobilising citizens to register for the ECOWAS biometric identity cards.[224] In Sierra Leone, the National Civil Registration Authority (NCRA) and the National Electoral Commission (NEC) carried out nationwide campaigns for the public to participate in the biometric civil and voter registration process prior to the March 2018 elections leading to the registration of 3.5 million citizens with technology from Smartmatic.[225]

222 *President Uhuru extends Huduma Namba registration deadline https://www.standardmedia.co.ke/nairobi/article/2001325962/uhuru-extends-huduma-namba-registration-deadline#:~:text=President%20Uhuru%20Kenyatta%20at%20a,will%20end%20on%20June%206.*

223 *IEBC To Suspend Voter Registration Exercise On Wednesday https://www.capitalfm.co.ke/news/2022/05/iebc-to-suspend-voter-registration-exercise-on-wednesday/*

224 *Coordination meeting - awareness campaign on cards November 6, 2019 http://dge.sn/fr/node/330*

225 *Civil and voter registration - Sierra Leone 2017 https://www.smartmatic.com/fileadmin/user_upload/CS_Sierra_Leone.pdf*

In Togo, the Regulatory Authority for Electronic Communications and Posts (ARCEP) and the Ministry of Digital Economy conducted a nationwide campaign for SIM card registration.[226] In 2021, the National Identification Agency of Togo (ANID) conducted a campaign to mobilise people to enrol for the country's biometric national identification project, e-ID Togo, which is expected to provide a unique ID number to all residents.[227] Similarly, in Lesotho, the campaigns were mainly focused on the process without providing details on the implication on peoples' right to privacy.

Non-state actors such as telecom companies have also conducted biometric data processing with limited public engagement. This was observed in the Central African Republic and the DRC, where these companies would only notify their customers of the requirement for SIM card registration without providing details of the scope of the data to be collected. For example, in DRC, Vodacom RDC in 2016 published a post on Facebook asking its subscribers to download and complete a SIM card registration form and send the form together with their national identity card to the operator's email address.[228]

The failure of some governments to be transparent and accountable by proactively disclosing information about the programmes only fuels suspicion, speculation, and scepticism among the public about the government's intentions, however noble the intentions are. Many biometric programmes fall within the Ministries of Interior, and are often classified as "national security" projects which add a thick cloud of secrecy around their design, procurement, cost and implementation. There is discontent in countries such as Nigeria, Kenya and Uganda over the investments in expensive and multiple bureaucratic biometric registration regimes introduced in the past three to five years. The programmes seek the same or similar information, and require the public to be physically present, queue for hours, travel long distances and register their biometric data.

However, there has been pushback from civil society, in Kenya, Senegal, Sierra Leone, Tunisia, Uganda and Zambia, who have challenged the introduction of biometric data collection programmes in the absence of comprehensive policy, legislative and institutional frameworks. In Senegal, for instance, civil society has criticised the biometric driving licence as illegal, costly, excessive, intrusive and dangerous,[229] while the mandatory SIM card registration was criticised for its non-compliance with the data protection law and the Commission of Personal Data (CDP) regulations.[230] In Sierra Leone, activists opposed legislative changes to make digital identity a requirement for voting in the 2023 elections. In Kenya, the mandatory government-led Huduma Namba digital identification project was challenged in court in 2019 on the grounds of interference with the constitutional right to privacy, lack of a data protection law and failure of the government to conduct a data protection impact assessment.[231]

In June 2017, the Uganda Communications Commission (UCC) ordered telecom operators to use subscribers' national identification numbers (NIN) to verify SIM cards. The move was condemned by civil society as the country was yet to adopt a privacy and data protection law that would have guided the process of data collection and sharing.[232]

226 *The Order limiting the number of SIM cards explained by ARCEP, Togo Cellulaire and Moov Africa Togo https://arcep.tg/larrete-portant-limitation-du-nombre-de-cartes-sim-explique-par-larcep-togo-cellulaire-et-moov-africa-togo/*

227 *Government prepares communication campaign for e-ID Togo project https://www.togofirst.com/en/public-management/0106-7945-government-prepares-communication-campaign-for-e-id-togo-project*

228 *Vodacom RDC https://web.facebook.com/VodacomRDC/posts/bonjour-chers-fanscliquez-sur-ce-lien-httpsdrivegooglecomfiled0b4fqidasrlpiy2llx/903542726420149/?_rdc=1&_rdr*

229 *Biometric Driver's License: An Illegal, Expensive, Excessive, Intrusive and Dangerous Project http://www.osiris.sn/Permis-de-conduire-biometrique-Un.html; Asutic: "The biometric driving license is dangerous and illegal" https://senego.com/asutic-le-permis-de-conduire-biometrique-est-dangereux-et-illegal_1010014.html*

230 *Quarterly Notice N° 01-2021 of the Personal Data Protection Commission of Senegal (CDP) https://www.cdp.sn/content/avis-trimestriel-n%C2%B0-01-2021-de-la-commission-de-protection-des-donnees-personnelles-du-0; https://cipesa.org/?wpfb_dl=291*

231 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR http://kenyalaw.org/caselaw/cases/view/189189/*

232 *Unwanted Witness Condemns the criminal use of citizens' bio data & calls on gov't to formulate safeguards to protect lives and property. https://www.unwantedwitness.org/unwanted-witness-condemns-the-criminal-use-of-citizens-bio-data-calls-on-govt-to-formulate-safeguards-to-protect-lives-and-property/*

3.2 Inadequate Legal Frameworks Heightening Risks to Privacy

A key risk to privacy is the implementation of digital biometric programmes in the absence of adequate or comprehensive policy, legal and institutional frameworks for privacy and data protection. This includes mechanisms to implement the principles of data protection such as data minimisation and consent, which are vitiated by the mandatory nature of the programmes. For instance, these frameworks are absent in Cameroon, the Central African Republic, the Democratic Republic of Congo, Liberia, Nigeria, Sierra Leone, and Tanzania. In countries where the laws are present, in some instances they are weak, fragmented, outdated, poorly enforced and do not provide strong and independent oversight mechanisms for data privacy protection or effective remedies, yet governments have intensified the deployment of data collection technologies such as CCTV with automated facial recognition technology.

Many governments do not have in place proper procedures or safeguards for the sharing of data between state institutions. In Tanzania, the data-sharing agreements between NIDA and other agencies are not disclosed to the public. In Senegal, the centralisation of databases and the lack of information about the levels of access to such databases also fuel fears of abuse of the data. Similarly, in Senegal, the lack of transparency around the unified biometric card used as a national identity card and a voter's card has fuelled speculation over possible abuse by politicians to target voters in specific areas.

In most of the countries where SIM card registration is mandatory, there is concern that service providers may be compelled under existing communication interception laws to aid state surveillance activities by providing information of subscribers to state security agents. This was witnessed in Togo where given the absence of a privacy law, three journalists Komlanvi Ketohou, Ferdinand Ayité, and Luc Abaki, were on a list of 300 persons potentially targeted for surveillance through their phones by clients of Israeli firm NSO Group using Pegasus spyware.[233] Countries like Morocco, Mozambique, Rwanda and Zambia, have been reported to operate Pegasus, while its infections have been reported in Algeria, Cote d'Ivoire, Egypt, Liberia, Uganda and South Africa.[234]

In Tunisia, the decades-old data protection law is outdated and is yet to be updated to reflect the current global trends and developments in data privacy. Generally, the absence of clear and robust regulatory frameworks in countries, opens up biometric systems to abuse of the rights of data subjects.

Majority of the countries studied have not ratified the 2014 African Union's Malabo Convention, which aims to guide member states in coming up with a harmonised legal regime on data protection. Only 14 countries are signatories and 13 have ratified out of 55 Member States, and these are Angola, Cape Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo and Zambia.[235] This implies that Africa is yet to embed a common regulatory approach to accelerate privacy protection and adopt a shared understanding of how to confront emerging threats to privacy in the digital era. Some of the benefits of common approaches such as the development of locally relevant tools, policies and guidelines; unified training content and capacity-building programmes; and technology and skills transfer, which have benefited jurisdictions like the European Union, could also be enjoyed in Africa.[236] The persistent craving for biometric data programmes in Africa must be complemented with appropriate policy, regulatory and institutional frameworks to safeguard the privacy of data subjects and protect their biometric data.

233 *'There is no private life': Three Togolese journalists react to being selected for spyware surveillance https://cpj.org/2021/09/togolese-journalists-spyware-surveillance/*

234 *How digital espionage tools exacerbate authoritarianism across Africa https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/*

235 *List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf*

236 *Surveillance Technology a Concern for many in Africa https://newafricadaily.com/surveillance-technology-concern-many-africa*

In Cameroon, Central African Republic, Democratic Republic of Congo, Liberia, Nigeria, Sierra Leone, and Tanzania there are no independent data protection authorities set up to oversee the collection and processing of data in the biometric data collection programmes. In Lesotho, the state is yet to establish its Data Protection Commission more than a decade after its Data Protection Act, 2011 came into force.[237] Further, the power to collect and process biometric data for essential services is fragmented across multiple laws and institutions operating in silos without clear or common frameworks to guide the design, implementation and deployment of such programmes. As a result, state and non-state actors continue to implement unregulated mass biometric data collection programmes in poorly managed systems and processes without taking responsibility for the potential privacy risks, while remaining opaque and unaccountable for their actions and the potential privacy breaches that might result.

The absence of effective legal frameworks and independent oversight, the use of centralised databases, weak information sharing safeguards, and the lack of transparency and accountability in the management of these databases are loopholes that inevitably create opportunities for abuse by state and non-state actors with access to the information.

3.3 Exclusion from Accessing Essential Services

Biometric data collection programmes such as digital IDs are implemented in societies with specific cultural, social, economic and political contexts, and these need to be considered in their design and the systems adapted to suit the context.[238] Otherwise, they may end up digitising pre-existing problems with existing identity management systems, some of which bear colonial relics, and historical discrimination. In the countries studied, registration for the biometric data programmes is often tied to an individual's possession of primary official identification documents such as national identity cards, birth certificates and driver's licences. Thus, a person's lack of such documentation could lead to their exclusion from accessing basic services including adult suffrage, financial services, employment, education, health, social services, travel, registering a business, SIM card ownership and consequently internet access.[239]

According to the World Bank's 2018 ID4D Global Dataset, 81% of the one billion people around the world who face challenges in proving their identity due to a lack of official identity documents are in Sub-Saharan Africa (494 million) and South Asia (312 million).[240] Further, women are more likely to lack an ID compared to men. This gap is higher in low-income countries where one in two women do not have official proof of identity.[241] According to the ID4D Global Dataset, the top 10 countries in Africa with the highest levels of unregistered populations in 2018 were Somalia (77%), Nigeria (72%), Eritrea (70%), Ethiopia (65%), Angola (56%), Zambia (56%), South Sudan (53%), Chad (53%), Equatorial Guinea (53%), and Uganda (49%).[242]

237 *Lesotho https://www.dataguidance.com/jurisdiction/lesotho*

238 *Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---soc_sec/documents/publication/wcms_631504.pdf; Identity in a Digital Age: Infratructure for Inclusive Development https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf; Digital ID 101: Making sense of key terminology https://www.africaportal.org/features/digital-id-101-making-sense-key-terminology/ ; Identity in a Digital World A new chapter in the social contract https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf*

239 *see for instance, No Gov't Service Without Huduma Card As Use Of National ID Ceases In Dec. 2021 https://www.citizen.digital/news/no-govt-service-without-huduma-card-as-use-of-national-id-to-cease-in-december-2021-646968*

240 *The global identification challenge: Who are the 1 billion people without proof of identity? https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity*

241 *ID4D Data: Global Identification Challenge by the Numbers https://id4d.worldbank.org/global-dataset*

242 *2018 Global Dataset https://datacatalog.worldbank.org/cee776e9-8c54-47dd-90bd-1163315183e8*

New programmes could also exacerbate historical injustices from colonial times associated with exclusion from access to legal identity. In Kenya, a case challenging the Huduma Namba project raised the aspect of digitalised discrimination which would affect members of Nubian and Somali communities who already faced additional scrutiny and hurdles in establishing their citizenship and applying for identity documents. They were now at risk of exclusion from accessing services due to lack of the Huduma Namba.[243] In 2016, Kenya had an estimated 18,500 stateless communities such as the Makonde, Shona, and Pemba who had lived in the country for more than 80 years without being recognised as Kenyans and as such had not been issued identification documents.[244] The government only recognised the 8,000 Makonde people in 2016 and the 3,500 Shona in 2021,[245] while around 4,000 Pemba await legal recognition to date.[246]

Similarly in Togo, many people lack basic legal identification such as birth certificates, national identity cards or passports, which denies them an opportunity to open bank accounts to access credit facilities, enrol children in schools, procure health insurance, benefit from social protection programmes or register their SIM cards.[247] The country's relief programme, Novissi - Programme de Revenu Universel de Solidarité, which was implemented following the COVID-19 pandemic, was criticised for requiring citizens to produce their voter cards before accessing relief services. The opposition made a public call to boycott the exercise since it would be exclusionary.[248]

In Uganda, there have been complaints that the biometric identification programme does not cover remote areas, forcing many in such regions to travel to urban areas to access services. Furthermore, the process of enrolment for national identity cards has excluded marginalised people on the basis of disability and ethnicity.[249] For example, persons with disabilities, such as those without hands, have been turned away for lack of fingerprints instead of being provided with an alternative mechanism Some ethnic minorities such as the Maragoli are not recognised as an ethnic group in Uganda and have been denied registration.[250] Other discriminatory practices include denial of access to registration due to long distances to registration centres, language barriers, and for lack of supporting documents such as marriage certificates.

Up to one-third of Ugandans in 2021 did not have a biometric ID card seven years after the system was introduced, thus excluding them from vital healthcare and social services[251] with women and elderly people mostly affected.[252] Moreover, the ID project locally referred to as "Ndaga Muntu" is viewed as a national security instrument, and the lack of identity could leave one to be deemed a foreigner. Some of the cards have been reported to have errors, where correcting mistakes or replacing the cards costs UGX 50,000 (USD 13.05), which is unaffordable to many. In March 2021, the government was sued for making it mandatory for citizens to produce their national identity cards or numbers (NIN) in order to access COVID-19 vaccination, which is pending determination.[253] Furthermore, the lack of the ID card has been identified as an inhibitor to opening bank accounts, buying SIM cards, acquiring passports, and gaining formal employment.

243 *Case Filed to Stop New Digital ID Register in Kenya https://namati.org/news-stories/case-filed-stop-new-digital-id-system-kenya/*

244 *Africa's invisible millions survive without ID documents https://www.equaltimes.org/africa-s-invisible-millions?lang=en*

245 *Joy as Kenya grants citizenship to stateless descendant of migrants from Zimbabwe https://www.fairplanet.org/story/joy-as-kenya-grants-citizenship-to-stateless-descendant-of-migrants-from-zimbabwe/; End of statelessness in sight for Shona as Kenya issues birth certificates https://www.reuters.com/article/us-global-rights-stateless-kenya-feature-idUSKBN1WN15Q*

246 *The Pemba Minority Stateless in Kenya https://ghrd.org/the-pemba-minority-stateless-in-kenya/*

247 *Togo hopes to launch new biometric ID card in 2021 https://www.biometricupdate.com/202012/togo-hopes-to-launch-new-biometric-id-card-in-2021*

248 *Togo: Fumbling With a Digital ID While Actively Surveilling Citizens https://cipesa.org/2022/04/togo-fumbling-with-a-digital-id-while-actively-surveilling-citizens/*

249 *Uganda: Are Digital IDs a Tool for Inclusion or Exclusion? https://researchictafrica.net/2021/06/23/uganda-are-digital-ids-a-tool-for-inclusion-or-exclusion/*

250 *Maragoli vs. Agribusiness and the Republic of Uganda https://indigenousafrica.org/the-maragoli-of-uganda/#:~:text=Despite%20having%20been%20present%20in,only%20to%20recognized%20%E2%80%9Ctribes%E2%80%9D.*

251 *FEATURE-Uganda sued over digital ID system that excludes millions https://www.reuters.com/article/uganda-tech-biometrics-idUKL3N2X32RG*

252 *Uganda's ID scheme excludes nearly a third from healthcare, says report https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report; Chased away and left to die https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf*

253 *Covid-19 vaccine: CSOs petition court challenging national ID requirement https://www.unwantedwitness.org/covid-19-vaccine-csos-petition-court-challenging-national-id-requirement/*

In Tanzania, the deactivation of SIM cards in 2020[254] and deregistration of cards suspected to have been used to commit crimes[255] denied many citizens access to the internet due to failure to re-register.

In Zambia, implementation of the nationwide new biometric identity registration process is yet to be achieved. In addition, the discrimination of women and girls in the country especially through traditional rules and practices constrains their access to and use of identity documents.[256] Further, the requirement for birth certificates in order to acquire the national registration cards, or the use of national registration cards to access healthcare SmartCare cards, financial services such as bank accounts and mobile banking, SIM card registration or voter registration, makes it difficult for women to access these services owing to their lower ownership level of these documents in comparison to men.[257] In 2016, Zambia had the fourth lowest birth registration for children under five years in the world with coverage standing at below 15%.[258]

3.4 Enhanced Surveillance, Profiling and Targeting

The use of CCTV with embedded facial recognition technologies is increasingly becoming more accessible and prevalent on the continent, yet these systems tend to be intrusive. These systems can track the movement of people, recognise motor vehicle number plates, and match live footage of people in the public with images of those on a 'watch list' based on their ability to recognise specific and unique facial features, akin to fingerprinting.[259]

There are several dangers posed by these systems in the African region. Firstly, they are implemented passively, collect indiscriminate footage of people, and do not require the knowledge, consent or participation of the data subjects, thus are less prone to suspicion.[260] The introduction of surveillance systems around the continent such as Huawei's Safe City and ZTE's Smart City Projects have been touted by governments as crucial for enhancing security. However, they have been criticised as representing threats to civil liberties and not delivering the promised dividends such as curbing crime and improving centralised city management.[261]

Secondly, where CCTV footage is combined with biometric data and biographical information captured from the mass digital identification programmes, they can create a potent surveillance tool that renders residents more vulnerable to targeted profiling, tracking, political surveillance and suppression.[262] Across the continent, commercial entities such as banks and telecos in Kenya are increasingly being provided with access to government databases to enable them to authenticate official documents. In addition, companies that develop biometric systems such as Zetes, Smartmatic, Huawei and ZTE are often co-opted as suppliers and implementers of projects. However, there is limited transparency and accountability by these entities including disclosure of the data sharing agreements outlining the nature and types of data shared, how it is used, and the people responsible for making decisions about it.

254 *Xinhua, "Tanzanian regulator locks out over 650,000 mobile phone users," The East African, January 21, 2020, https://www.theeastafrican.co.ke/tea/news/east-africa/tanzanian-regulator-locks-out-over-650-000-mobile-phone-users-1435268*

255 *Sharon Sauwa, "18,000 SIM cards blocked in Tanzania," The Citizen, July 29, 2021, https://www.thecitizen.co.tz/tanzania/news/national/18-000-sim-cards-blocked-in-tanzania-3490770*

256 *Digital Identity Country Profile: Zambia https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Zambia.pdf*

257 *Digital Identity Country Profile: Zambia https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Zambia.pdf*

258 *Identification for Development (ID4D) Identification Systems Analysis: Country Assessment Zambia https://openknowledge.worldbank.org/bitstream/handle/10986/25106/108360.pdf?sequence=4&isAllowed=y*

259 *Collection of Biometric Data and Facial Recognition https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/collection-of-biometric-data-and-facial-recognition/*

260 *Facial recognition technology https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology*

261 *Beyond the Digital Cold War: Western, Eastern and Southern Tales of Digital Failure and Success https://www.cigionline.org/articles/beyond-the-digital-cold-war-western-eastern-and-southern-tales-of-digital-failure-and-success/*

262 *Surveillance Technology a Concern for many in Africa https://newafricadaily.com/surveillance-technology-concern-many-africa*

In most of the countries reviewed, SIM card registration is mandatory and is linked to civil registration data such as national identity cards which are used for verification of identity prior to registration. In addition, as part of the registration process, subscribers are required to provide comprehensive biometric and biographical information about themselves. This information is provided to telecoms and can in some cases be accessed by local regulators and state agencies on request, in some instances without robust judicial oversight. The key risk is that information obtained from SIM card registration including cell phone geolocation data when cross-referenced with civil registry databases and live feeds from CCTV cameras with facial recognition capability, could be used for surveillance and triangulation of the location of state targets.

In many countries where these new biometric data collection programmes are being launched, key reasons for their introduction include to safeguard national security and fight crime. However, as noted above, in a number of these countries, there are weak safeguards to the privacy of the data, and thus abuses are perpetrated by the absence of independent oversight. Indeed, there are legitimate fears of function creep where authoritarian governments hijack these digitisation programmes and use the information collected legitimately to achieve purposes that were otherwise unintended, and which are unregulated with no clear procedures or oversight. For example, civil registration data can be used to check information against criminal databases, validate SIM card registration, and for the verification and authentication to access financial services, voter registration, and for health care insurance provision.

In Angola, DRC, Mozambique, Nigeria and Uganda, CCTV surveillance, SIM card registration and the national identity card added to fears of the same being used to profile, monitor, track and arrest government critics, journalists, protesters and opposition leaders.[263] Following the #EndSARS campaign in Nigeria in October 2020, some protesters like Bolatito Oduala, popularly known as Rinu, and 19 others were tracked and their bank accounts frozen by the Central Bank of Nigeria (CBN) and accused of money laundering and terrorism. Also, Modupe Odele, who provided legal aid to protesters, had her international passport seized by the Nigerian Immigration Service (NIS) while on her way to the Maldives. In Uganda, following anti-government protests in November 2020, police used images from the CCTV surveillance system to track down and arrest more than 836 persons suspected to have participated in the protests.[264]

3.5 Conflicting Interests and the Power of Third Parties

The development and deployment of identity management systems have largely been led by private sector companies, with various multilateral organizations, companies, international NGOs and foreign donors providing loans and technical support. Some of the associated risks include increased dependency on proprietary systems provided by certain suppliers who are sometimes retained at exorbitant costs, the hosting of critical databases outside the country's jurisdiction, and lack of technology and skills transfer after deployment. This often leaves the implementing government agencies at the mercy of suppliers as they have limited control of their information and systems. The use of proprietary systems, as opposed to open-source ones, can also affect the ability of governments to contract different service providers. In Kenya for example, Smartmatic International which was contracted by the elections body, IEBC, refused to grant access to server images citing infringement of its intellectual property rights, despite a court order issued by the Supreme Court in August 2022.[265]

263 *(ngali – Surveillance of public spaces and communications in the DRC (The Media Policy and Democracy Project, P. 8): https://www.mediaanddemocracy.com/research.html*

264 *Ugandan police accused of using facial recognition system to fuel rights abuses*
https://www.biometricupdate.com/202011/ugandan-police-accused-of-using-facial-recognition-system-to-fuel-rights-abuses

265 *Kenya poll petition: Smartmatic declines to open IEBC servers to Raila Odinga*
https://www.theeastafrican.co.ke/tea/news/east-africa/smartmatic-declines-to-open-iebc-servers-to-raila-odinga-3933676

In addition, there have been concerns about the role of Chinese companies such as Huawei and ZTE in Europe and the US about the ramifications of their involvement in the development of new 5G networks over accusations of installing backdoors used to spy on behalf of the Chinese government, which the companies have denied.[266] Similarly, there is concern in Africa as Huawei is reported to have built about 70 per cent of Africa's 4G networks is accused of selling to African governments, potentially repressive technologies as part of the Safe City initiative which technologies could undermine human rights.[267] These security concerns have been overshadowed by the demand for internet access in the continent and the absence of cheaper alternatives.[268]

Concern has also been raised by civil society regarding the use of aid from the European Union in West Africa for the development of legal identity and surveillance programmes in several countries as part of a broader mission towards migration control.[269] In November 2020, civil society organisations condemned the use of EU aid and cooperation programmes to train and equip security forces in Africa with surveillance techniques.[270] A report by Privacy International revealed that the European Union Agency for Law Enforcement Training (CEPOL) had trained police and security agencies in Algeria, Morocco and Tunisia in phone and internet surveillance, including social media monitoring, telecommunications metadata analysis, device investigations and data extraction.[271] It was further reported that border and migration authorities in Algeria, Egypt, Niger, Libya, Morocco, and Tunisia, had undergone similar training and were provided with technical equipment.[272]

The EU has supported the ECOWAS Commission with USD 24 million to build its capacities in migration data management, border management, labour migration and counter-trafficking.[273] It has also supported the Senegalese government with USD 27 million for the development of biometric digital identification systems through the "Emergency Trust Fund for Africa".[274] Part of support to Niger from the Fund included USD 11.1 million for the provision of surveillance drones, surveillance cameras, surveillance software, a wiretapping centre, and an international mobile subscriber identity (IMSI) catcher.[275] Cote d'Ivoire was allocated EUR 29 million towards the development of its universal biometric identity system to enable the identification of Ivorians irregularly residing in Europe in order "to organise their return more easily".[276]

The World Bank under the West Africa Unique Identification for Regional Integration and Inclusion project has provided USD 273 million to support ECOWAS states such as Benin, Burkina Faso, Côte d'Ivoire, Guinea, Niger and Togo to implement foundational identification systems.[277] Phase one of the e-ID projects started in 2018 with Côte d'Ivoire and Guinea at a cost of USD 395.1 million.[278]

266 *Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/*

267 *Ibid*

268 *For Africa, Chinese-Built Internet Is Better Than No Internet at All https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/*

269 *The EU's next budget is a huge threat to privacy - here's what must be done https://privacyinternational.org/advocacy/2548/eus-next-budget-huge-threat-privacy-heres-what-must-be-done; Border Management Programme for the Maghreb region (BMP-Maghreb) https://ec.europa.eu/trustfundforafrica/sites/default/files/t05-eutf-noa-reg-07.pdf*

270 *Civil Society Groups Denounce the European Union's Involvement in Surveillance in Africa https://cipesa.org/2020/11/civil-society-groups-denounce-the-european-unions-involvement-in-surveillance-in-africa/*

271 *ere's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric*

271 *Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border*

273 *ECOWAS launches a 26-million € EU-Funded project on migration https://www.ilo.org/africa/whats-new/WCMS_242035/lang--en/index.htm*

274 *EU Emergency Trust Fund for Africa https://bit.ly/3SIQsZM; CIVIPOL https://bit.ly/3Px6OSI*

275 *Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border*

276 *The Future of the EU Trust Fund for Africa https://privacyinternational.org/sites/default/files/2019-09/EUTF%20Policy%20Briefing.pdf*

277 *Togo, Benin, Burkina Faso and Niger Join West Africa Regional Identification Program to Help Millions of People Access Services https://www.worldbank.org/en/news/press-release/2020/04/28/togo-benin-burkina-faso-and-niger-join-west-africa-regional-identification-program-to-help-millions-of-people-access-services*

278 *Ibid*

Notably, all countries or private entities whether European, Chinese, or American involved in biometric data projects are keen to advance their own political, technological or commercial interests, which may come at the cost of individuals' privacy. Therefore, it is critical for African countries in their engagement in such partnerships to beware of the emerging data colonisation and vendor lock-in, and instead prioritise the adoption of systems that do not compromise privacy and data protection at the altar of personal, political, commercial or other interests.

3.6 Limited Capacity and Training

Where data protection authorities have been established like in Ghana, Kenya, Uganda and Zambia, they are relatively in their infancy and lack the institutional and financial independence to effectively discharge their mandate. In addition, they are not adequately resourced and heavily rely on their parent ministries for staff and budgets, which also affects their work. Moreover, national security exemptions in national laws shield state security agencies from scrutiny and accountability by data protection bodies, contributing to further abuses of biometric data.

In addition, in countries such as the Central African Republic, Kenya, Sierra Leone and Uganda, the competence of the staff of state institutions responsible for biometric data collection was noted by respondents to be a challenge. In the Central African Republic, some of the staff are not well trained on effective ways to safeguard the privacy of users' information during the data gathering processes such as for voter registration purposes. In Sierra Leone, some of the personnel in these institutions can hardly appreciate the required personal data ethics in the discharge of their duties. In Kenya and Uganda, some of the personnel had difficulties operating the digital devices used to collect biometric data.

250 *Global Freedom Score 2022 https://freedomhouse.org/countries/freedom-world/scores*
251 *Internet Freedom Score 2021 https://freedomhouse.org/countries/freedom-net/scores*
252 *Global Freedom Score 2022 https://freedomhouse.org/countries/freedom-world/scores*
253 *Internet Freedom Score 2021 https://freedomhouse.org/countries/freedom-net/scores*

4.0 Conclusion and Recommendations

4.1 Conclusion

This report has reviewed the developments in biometric data collection and processing in 16 countries in Africa. It covers the emerging and ongoing practices by governments in the digital civic space. The specific areas of focus include the deployment of national biometric technology-based programmes and the mode of implementation, the associated gaps and challenges as well as the risks posed to data protection and privacy and other digital rights.
Advancement in technology comes with multiple benefits, challenges and risks. Africa has undergone exponential growth in technology, which has birthed several digital transformation programmes. Consequently, technology-based biometric data collection programmes have become attractive for governments seeking to digitise their civil registration and e-government services and grow their economies.

There is a growing appetite by countries to upgrade and incorporate biometric data collection in population databases for foundational identification systems, elections, healthcare, immigration, education, social protection, financial institutions, refugee registration and national security systems for real-time surveillance. Likewise, as biometric technologies become more ubiquitous, they are also becoming more sophisticated, relied upon and gaining more use cases across a variety of applications within society, each with a significant human rights impact.
While biometric data collection under various programmes can bring several benefits, it can also cause harm given the risks it poses that threaten personal data and privacy. Biometric data, unlike other forms of data used for authentication like passwords and codes, cannot be changed or edited. It remains the same for the duration of a person's entire life, thus ensuring the security of biometric data is critical. These programmes will be expected to collect and process sensitive personal data of much of Africa's 1.4 billion people, yet the investments in the legal, technical, regulatory and procedural privacy safeguards to secure the information and the measures to mitigate the harm and negative effects are largely insufficient.

Biometric data collection systems rely on internet connectivity, computer networks, and digital devices and databases for effective implementation of key functions such as registration, identification, authentication and verification of identity. The key risks to the security of these systems include hacking and data breaches, cyber attacks, identity theft and fraud. These risks could be aggravated where the data is stored in centralised databases and where there are inadequate information security policies, procedures and practices. This is especially so where the databases are interconnected with other government agencies and linked to provide convenience in services such as authentication for financial services, elections, SIM card registration, or provision of social services, without due regard to the consequences of widespread data sharing or evaluation of the risks to the privacy of the information.

Additionally, even in the 30 countries with data protection and privacy laws, the laws are weak with inadequate oversight mechanisms and institutions to comprehensively protect individual privacy, while the remedies in case of a breach are ineffective and often unknown to the average data subject. Many countries do not have specific privacy and data protection laws, which means that the right to privacy and protection of personal data can not be effectively ensured.

The right to privacy is essential in a democratic society as it plays a critical role in the realisation and enjoyment of the rights to freedom of expression, association, assembly and access to information. In the Global Freedom Score 2022, Angola, Cameroon, the Central African Republic, and the Democratic Republic of Congo are rated as "Not Free" while Lesotho, Liberia, Kenya, Mozambique, Nigeria, Senegal, Sierra Leone, Tanzania, Togo, Tunisia and Zambia are rated as "Partly Free". Further, Angola, Kenya, Nigeria, Tunisia, Uganda and Zambia are rated as "Partly Free" by the Internet Freedom Score 2021. Moreover, the internet privacy index which details the extent to which countries have taken steps to protect privacy online, ranked Tunisia highest among the African countries included in the assessment at 45 out of 110 countries surveyed. It was followed by Senegal (54), Kenya (57), Liberia (69), Nigeria (79), Zambia (84), Sierra Leone (85), Tanzania (88), Uganda (89), Togo (91), Angola (93) Mozambique (100) and Cameroon (102). The Central African Republic, the Democratic Republic of Congo and Lesotho were not ranked. From the foregoing, it is apparent that most countries under review are mostly ranked dismally as they have some of the lowest levels of protection of political rights, civil liberties, internet freedom and privacy.

Consequently, the implementation of biometric programmes in countries with poor digital rights records, declining democracy and rising digital authoritarianism fails to inspire confidence and casts doubt on the integrity of biometric databases data collection programmes shall be maintained and be free from abuse. Such databases, despite their high cost of implementation, can also create incentives for identity theft, discrimination, and exclusion from access to services. However, centralising, consolidating and linking information collected in national biometric digital databases with individuals' information harnessed from digital ID programmes, CCTV cameras with facial recognition, mandatory SIM card registration, in environments with weak privacy laws and pervasive communication surveillance laws and insufficient oversight is a growing problem. Viewed collectively, the developments, trends and risks outlined in this report can only heighten concern over the growing threats to the right to privacy of personal data and potential violations of digital rights on the continent.

4.2 Recommendations

This section presents recommendations to various stakeholders including the government, civil society, the media, private sector and academia, which, if implemented, will go a long way in addressing data protection and privacy gaps, risks and challenges in the study countries.

Government

- Implement the laws and policy frameworks on identity systems and data protection and privacy while paying keen attention to compliance with regionally and internationally recognised principles and minimum standards on data protection and privacy for biometric data collection and require the adoption of human rights-based approaches. These laws and policies should be reviewed regularly and future-proofed to address the challenges of technological innovation.
- Countries without data protection and privacy laws such as Liberia, Mozambique, Sierra Leone and Tanzania should expedite the process of enacting appropriate data protection laws so as to guarantee the data protection and privacy rights of their citizens. The process of enactment of such laws should pay attention to, and align the legislation with the regionally and internationally accepted data protection principles and practices to cover the entire data lifecycle.
- Establish independent and robust oversight data protection bodies to regulate data and privacy protection including biometric data. The bodies should be given a commendable level of autonomy and facilitated sufficiently with the required resources to ensure that they function effectively, independently and with minimal external influence over their mandate. They should be empowered to enforce the laws, receive and investigate complaints, carry out routine compliance checks and rigorously monitor the conduct of data protection audits and human rights impact assessments at every stage of proposed and ongoing biometric data collection programmes.

- Study countries especially Algeria, Botswana, Cameroon, Egypt, Ethiopia, Ivory Coast, Kenya, Liberia, Madagascar, Morocco, Nigeria, Sierra Leone, South Africa, Tanzania, Tunisia, Uganda and Zimbabwe, should swiftly ratify the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The Malabo Convention is a key guiding instrument on harmonising and strengthening existing and incoming national cyber legislation in Africa. Ratification will show commitment to the protection of data protection and privacy including of biometric data, cyber security and the information society.
- Build the capacity of government officials responsible for biometric data collection programmes, including data protection bodies, law enforcement, prosecution, regulators, and the Judiciary in effective data protection. Capacity building can extend to skilling them in compliance with principles of data protection and the rights of data subjects. This will buttress data protection and ensure appropriate and lawful handling of personal data.
- Promote continuous and meaningful public consultations and multi-stakeholder engagements with key stakeholders such as civil society, the private sector, academia, the technical community and the media on data protection and privacy including biometrics. Such engagement, when buttressed with proactive disclosure of information prior to the inception and continuously during the implementation of biometric programmes, can be instrumental in promoting transparency, addressing discrimination, developing appropriate solutions, building trust and eliminating misconceptions and suspicions regarding the implementation of biometric systems.
- Take deliberate efforts that aim to promote inclusion and eliminate barriers leading to exclusion and inequality faced by the vulnerable, marginalised and minority groups including persons with disabilities, women, youth, people living in low-income areas and rural communities, elderly, sexual minorities, migrants and refugees in the provision of essential social and economic services using justifications such as non-acquisition of legal identity documentation like birth certificates, national identity cards and passports and failure to enrol in national biometric data collection programmes as basis for denial of services. Also, complementary or alternative means of identification should be acceptable to access essential public services.
- Prior to the implementation of biometric programmes, governments should invest in conducting preparatory activities such as needs assessments, feasibility studies, pilot testing, training and capacity building, and public awareness programmes which can inform the design, choice and type of technologies that are appropriate and relevant to the context. The timing of these activities should be well planned, and the funding secured and procurement done on time to avoid delays and other implementation challenges.
- Promote the use of open design of systems and implementation standards to ensure interoperability, and avoid vendor-lock in order to promote competition in procurement, reduce costs and ensure flexibility.
- Conduct due diligence and risk assessments on suppliers of biometric technologies prior to their procurement to ensure their products, processes and services comply with applicable human rights standards.

Civil society

- Work hand-in-hand with other stakeholders including the government, private sector, technical community, media and the public to promote understanding and demystification of biometrics such as through awareness raising and building the capacity of key players in data protection and privacy. Such partnership can enhance the understanding and skills and competencies to respond to data protection and privacy emerging issues, challenges and opportunities.
- As human rights watchdogs, engage in advocacy and lobby governments to develop, implement and enforce privacy and data protection policies, laws and institutional frameworks that are in compliance with regional and international minimum human rights standards.
- Specifically push governments to ratify the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) to ensure government commitment to regional data protection and privacy as a means to hold them accountable.
- Monitor, document and report on the risks, threats, abuses and violations of privacy and human rights associated with biometric data collection programmes, and propose effective solutions to safeguard rights in line with international human rights standards.
- Constantly report cases of data protection and privacy violations to international human rights mechanisms such as the Universal Periodic Review (UPR) and the African Commission on Human and Peoples' Rights (ACHPR). Constant and progressive reporting can potentially lead to positive change since they are key to assessing the human rights record of the subject country. It is also a tool for enhancing accountability and transparency of the state which has acted in violation.
- Engage in strategic and collaborative public interest litigation in national and regional courts to challenge data and privacy violations by state and non-state actors with the aim of holding them accountable and getting effective remedies for aggrieved individuals or data subjects.

Media

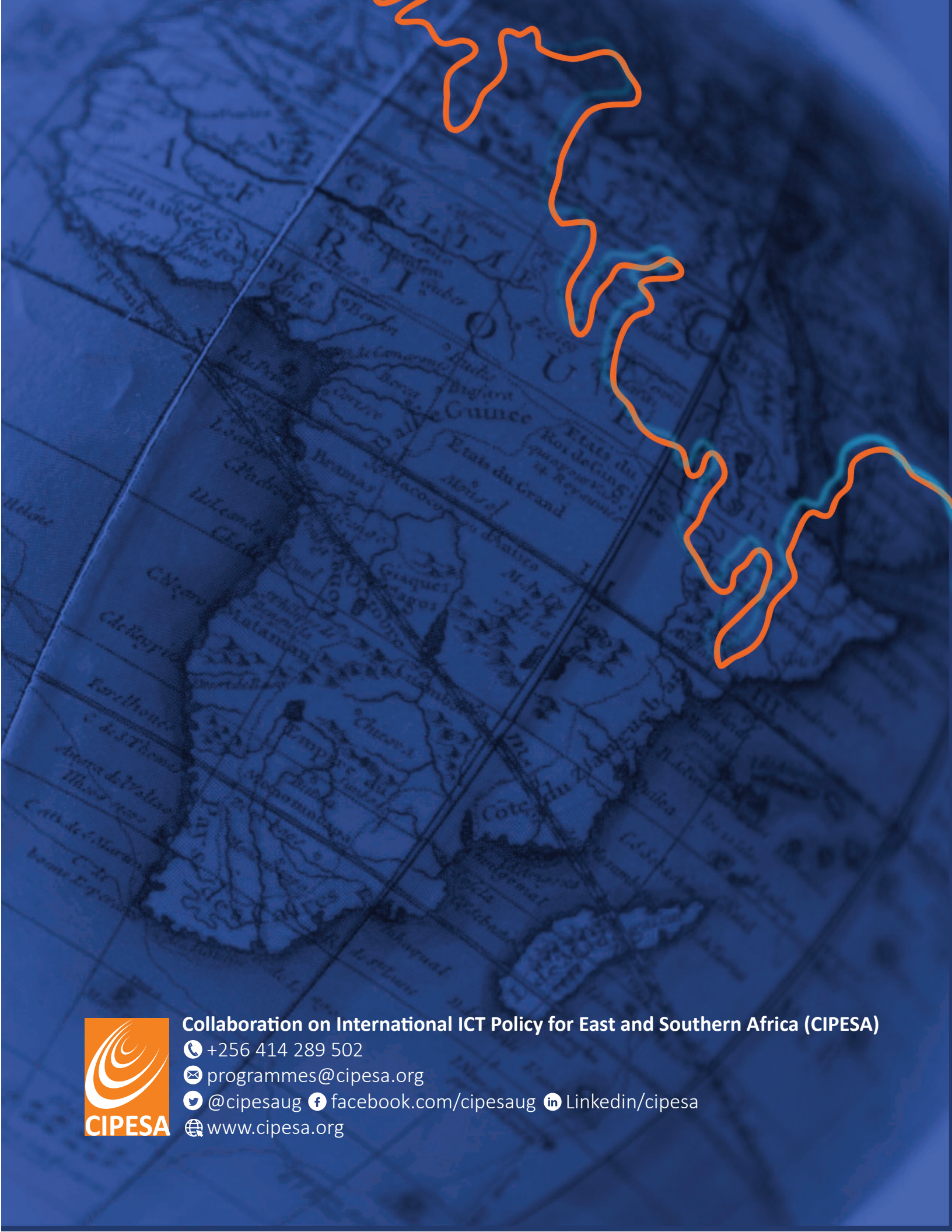
- Progressively document, report and publish initiatives such as advocacy and by civil society and other stakeholders to keep track of developments. Continuous engagement by the media can act as a tool for reflection and tracking accountability and transparency by the primary duty bearer - the government - in data protection and privacy.
- In collaboration with other stakeholders such as civil society, private sector and academia, raise awareness of the public with factual and objective information through increased coverage of the challenges, risks, threats, opportunities, benefits and implications of biometric data collection programmes and their impact on their privacy and other human rights.
- Conduct investigative journalism to identify and expose privacy violations arising from the implementation of biometric data collection programmes. Investigative journalism has the potential to enhance accountability and transparency in data protection and privacy.
- Build the capacity of journalists such as through tailor-made training in understanding data protection and privacy and effective reporting on this subject. The capacity building could potentially enhance journalists' understanding, monitoring and reporting of developments and trends in biometric data collection programmes, which in turn leads to effective coverage of issues.

Private sector

- Take deliberate efforts to ensure that all their respective biometric data collection programmes and systems are developed, implemented and managed in compliance with best practices prescribed by the national, regional and international human rights standards and practices on privacy and data protection, including the UN Guiding Principles on Business and Human Rights.
- Ensure that they progressively adopt and develop comprehensive internal privacy policies to guide the collection, storing and processing of personal data. Internal data protection policies will, through initiatives such as data privacy impact assessments, ensure transparent and accountable handling and management of personal data.
- Take deliberate efforts aimed at involving data subjects in the control and management of their personal data by providing timely information on external requests for information. This could potentially enhance public participation and remove cases of suspicion and mismanagement of personal data.
- Strongly stand against any unlawful personal data requests and practices from governments and frequently publish transparency reports. This will potentially build trust and confidence in the private sector and also enhance accountable and transparent management of personal data.
- Progressively adopt people-centred privacy, and privacy and security by design in the development and implementation of systems so as to place control over personal data in the hands of data subjects.
- In collaboration with other stakeholders like civil society, the academia and the media, support capacity building of policy makers to understand challenges, risks, and opportunities and implications of biometric data collection programmes geared toward the development of effective and progressive policies, laws on data protection and privacy.
- Create a prompt response mechanism for their clientele to any cases of data breaches, and continuously engage in awareness and education programmes for the public through the proactive publication of important information. This will potentially enhance public trust and understanding of the interplay of data protection and privacy and the associated data collection programmes.

Academia

- Conduct evidence-based research on data protection and privacy including biometrics highlighting the challenges, risks, benefits and trends in biometric data collection programmes. The research, once widely disseminated, can inform debate, litigation and advocacy for reform and progression across various frontiers such as the international human rights monitoring mechanisms.
- Collaborate with other key stakeholders and engage in initiatives which enhance, protect and promote data protection and privacy rights. Such initiatives include advocacy such as litigation and publication and building the capacity of the key stakeholders through training.
- Participate and input in policy and legislative development of data protection and privacy regimes by undertaking timely intervention in the processes. Timely intervention can be realised through direct provision of comments on the draft policies and laws as well as providing guidance on the content, shape and direction of data protection and privacy-centred policies, laws and instruments.



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
+256 414 289 502
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org