Biometrics and Digital Identity in Africa

Challenges, Opportunities and Policy Options

April **2024**

CIPESA

Introduction

Africa has witnessed an accelerated appetite for collecting and processing citizens' biometrics as countries transition from paper-based to digital identities. Biometric features such as fingerprints, the face, and the iris have become critical forms of authentication in issuing different identities, including birth certificates, passports, and national identity cards. The importance of digital identities in promoting trust and transparency for Africa's growing digital economy has been well articulated in the African Union's Digital Transformation Strategy for Africa (2020-2030)[1] and the African Continental Free Trade Area (AfCFTA).[2]

Globally, goal

16.9

of the United Nations Sustainable Development Goals (SDGs) provides an ambitious target of providing legal identity for all, including birth registration, by 2030.

Globally, goal 16.9 of the United Nations Sustainable Development Goals (SDGs) provides an ambitious target of providing legal identity for all, including birth registration, by 2030. However, in many countries, the enabling legal and policy framework is weak, with some countries lacking specific data protection laws and those with specific laws often lacking robust data protection standards. This renders the protection of the massively harvested and processed personal biometric data insufficient and exposed to risks such as identity theft and unregulated state surveillance.

The African Union (AU) has issued several instruments and guidelines, such as the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)[3] and the AU Data Policy Framework.[4] These instruments call upon Member States to only process personal data involving biometric data after authorisation by the relevant protection authority and to create a legal environment that enables the attainment and maximisation of the benefits of a data-driven economy. Several African countries are implementing biometric digital identity systems, spurred by technological advancements that have accelerated digitisation of processes and services. Such services include e-government, e-identification or digital identification, e-commerce, and digital banking. While the goals of Biometric Digital Identification (BDI) sometimes differ based on contexts and needs, the overriding purpose is to establish secure, reliable, efficient, and inclusive ways to identify and verify individuals in the digital age,[5] promote national security, stability, and efficient identity information management.[6]

In this brief, we discuss some of the critical drivers of BDI, the associated challenges, opportunities, and policy options for African countries. The brief offers recommendations for African countries to leverage the socioeconomic and political dividends of biometric digital identification without compromising citizens' fundamental rights to privacy, personal data protection, and other civil liberties.

[1] *AU Digital Transformation Strategy for Africa (2020-2023) https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf*

[2] *Africa Continental Free Trade Agreements (AfCFTA) https://au-afcfta.org/*

[3] *AU Convention on Cybersecurity 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*

[4] *AU Data Policy Framework https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf*

[5] *Global Report - Biometrics and Digital Identity: Trend Analysis and Comparative Assessment https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf*

[6] *State of Internet Freedom in Africa 2022 https://cipesa.org/wp-content/uploads/2022/09/State-of-Internet-Freedom-in-Africa-2022.pdf*

Drivers of BDI Collection Programmes

The collection and processing of biometric data over the past decade has been driven by several factors, including technological advancements, national security justifications, and improved modes of government service delivery.

Improving Service Delivery

Governments' appetite for collecting biometric data has partly been driven by the need to transform service delivery and enhance public participation through developing central databases. Since data is central to planning and economic transformation, the adoption of biometric data and digital identities is one way of improving efficiency in service delivery. Critical government programmes that have necessitated the collection and processing of biometrics include civil registration, issuance of National Identity cards, updating and verification of biometric voter's rolls, national e-passport initiatives, refugees' registration, and mandatory SIM card registration. This has driven the demand and adoption of digital identity (ID) credentials.[7]

Push for Regional Integration and Cross-Border Trade

The desire to harmonise and ease the cross-border movement of people and services has seen the adoption of various regional initiatives that require the collection and processing of personal data, including biometrics. For example, in July 2016, the AU unveiled the continent's first electronic passport to ease movement between countries. While this has yet to come to pass, several countries and economic blocs have embraced the concept and introduced e-passports for their citizens, which can store the biometrics of the passport holder.

For example, the Economic Community of West African States (ECOWAS) launched the "ECOWAS Card" in 2016 as a standard biometric identity card that could also be used as a travel document for citizens of its 15 member states. The move would also support the establishment of foundational identity databases that would be used as authentic references for other services such as the issuance of passports, driver's licenses, voter's cards, and social security cards.[8] Similarly, in April 2017, the East African Community (EAC) Council of Ministers directed Partner States to commence the issuance of the new EAC e-passport. The target was to have the old passports phased out by November 2022.

Both the African Union's Data Policy Framework and the Digital Transformation Strategy for Africa (2020-2030) provide additional catalysts for countries to embrace digital identities, including creating an enabling legal environment to maximise the benefits of a data-driven economy by encouraging private and public investments necessary to support data-driven value creation and innovation.

[7] *State of Internet Freedom in Africa 2022 https://cipesa.org/wp-content/uploads/2022/09/State-of-Internet-Freedom-in-Africa-2022.pdf*

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

Technological Advancements

Recent technological advancements have accelerated the adoption of BDIs, which are considered more authentic, secure, and reliable than paper-based identifiers. As technology becomes more accessible and affordable, governments and private entities continue to leverage biometric systems for functional and foundational ID purposes, and for an expanding array of applications.[9] A critical component has been the advancement within the Identity Management Systems (IDMS) and growing demand from both state and private entities for interoperability, allowing seamless integration between systems, applications, platforms, and information technology infrastructure.[10] In Uganda, for example, the country's electoral body, the Independent Electoral Commission (IEC), was able to extract relevant data, including biometric data and demographic information, such as polling stations, from the national identification register under the stewardship of the National Identity Registration Authority (NIRA), to compile the national voters' register during the 2016 elections.[11] The NIRA database was generated through a mass registration exercise as part of the National Security Information Systems (NSIS) project under the leadership of the Ministry of Internal Affairs, with the main aim of creating a centralised register that has all citizen data such as including photographs, names, date of birth, parents' data, location (that is, the district, county, sub-county, parish, and village), and fingerprints.[12]

In addition, the proliferation and adoption of mobile biometric solutions, including their multi-factor authentications (MFA) which is a multi-step system of securing data and applications where users are required to present a combination of two or more credentials to verify a user's identity for login. The MFA adds an extra layer of security such that even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or databases.[13] The confidence in MFA has accelerated faster ID enrolment and verification since, for the majority of the users, effective participation in any digitisation programmes involving the processing of their personal data depends on their perception and confidence that the data is secure and free from misuse.[14]

The emergence of generative Artificial Intelligence (AI) has also played a critical role in providing a supporting anchor for companies to incorporate new technologies, such as fingerprint or facial recognition, to support easy access and secure customer data as a way of enhancing remote identification and verification of users in a bid to improve user experiences.[15] Many users are encouraged to have their biometrics processed with the promise of seamless access to services in the comfort of their homes, without the incumbrances of physical presence.

[9] *Global Report - Biometrics and Digital Identity: Trend Analysis and Comparative Assessment https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf*

[10] *Ibid*

[11] *Integrating ICT in Elections: How Uganda Implemented Biometric Voter Registration, 2001–2016 https://www.kdevelopedia.org/asset/99202207120168788/1657590791650.pdf*

[12] *Ibid*

[13] *Multifactor Authentication https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication*

[14] *Digital Identity in a New Era of Data Protection https://unctad.org/meeting/digital-identity-new-era-data-protection#:~:text=The%20United%20Nations%20Sustainable%20Development,to%20prove%20who%20they%20are.*

[15] *How Biometrics Are Transforming the Customer Experience https://hbr.org/2023/03/how-biometrics-are-transforming-the-customer-experience*

Challenges to BDIs in Africa

18 of the 55

countries are still to enact comprehensive privacy and data laws.

In their current state, BDI programmes pose many challenges and risks to data subjects, including state-facilitated mass surveillance, data breaches, identity theft, and exclusion due to significant loopholes within the enabling legal environment and implementation processes. Several of the existing 37 national data protection laws in Africa are not robust enough, nor do they provide water-tight safeguards such as independent oversight bodies. The regulatory framework governing the processing of biometrics remains fluid, with several governments across the continent relying on scattered legal provisions to process biometrics and to mandate SIM card registration, voter registration, and issuance of national identification. The legal framework providing for the protection of personal data has remained insufficient as 18 of the 55 countries are still to enact comprehensive privacy and data laws.

In countries that have enacted data protection laws, most of them, such as Law No. 18-07 of 2018 on the protection of personal data for Algeria,[16] Kenya's Data Protection Act 2019,[17] Angola's Data Protection Act of 2011, Ivory Coast's Data Protection Law of 2013, and Uganda's Data Protection and Privacy Act of 2019[18] have weak safeguards. These laws often contain vague provisions regarding circumstances under which sensitive information can be accessed. Additionally, they rely on controversial narratives such as safeguarding national security, public interest, law enforcement, and criminal investigations to justify data access. This lack of clarity in the personal identity and biometric data laws creates room for ambiguity, misinterpretation,[19] and abuse.

Secondly, the prevalence of weak and outdated legal and institutional frameworks for civil registration which do not cater to BDI systems in countries such as the Central African Republic (CAR) and Mozambique, whose laws were last updated in 1964 and 1967, respectively, while others such as Angola, the Democratic Republic of Congo (DRC), Tanzania, and Uganda have had their laws amended within the last fifteen years have resulted in the reduction of trust in ongoing data processing programmes.[20] The lack of comprehensive legislative and governance structures, such as independent oversight and redress mechanisms, also exacerbates surveillance, data protection, and cybersecurity concerns. Independent oversight bodies play a critical role in the design, implementation, and operation of digital ID systems, including defining what is permissible or prohibited regarding the processing and sharing of personal data and biometric information, outlining ID users' consent, control, and rights, defining the scope of identity verification and authentication, establish oversight bodies or regulatory authorities.[21]

[16] *Article 18*

[17] *Part V (section 44-47)*

[18] *section 9*

[19] *https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf*

[20] *Global Report - Biometrics and Digital Identity: Trend Analysis and Comparative Assessment https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf*

[21] *Global Report - Biometrics and Digital Identity: Trend Analysis and Comparative Assessment https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf*

Thirdly, there is a growing concern across the continent where service providers are required under existing communication interception laws and or cybercrimes laws to aid state surveillance activities by providing subscribers' information to state security agents. In countries such as Cameroon, Rwanda, Uganda, Zambia, and Zimbabwe, intermediaries such as telecom companies and Internet Service Providers (ISPs) are required to facilitate surveillance, including by installing equipment and software that enable governments to lawfully intercept communications on their networks, including in real-time for such periods as may be required.[22] The assistance rendered by intermediaries facilitates targeted internet disruptions, easy access to users' data, content removals, decryption of users' encrypted data, and state surveillance[23] based on geolocations of the users.

Fourthly, the slow-phased way these programmes are implemented has resulted in non-documented citizens, especially in rural or hard-to-reach areas, the elderly, and persons with disabilities. In many countries, citizens have had to travel long distances and multiple times, in some instances, to complete their registrations due to poor infrastructure, such as roads and the Internet, malfunction of the kit, and lack of reliable electricity. Because possession of BDIs has become a prerequisite for service delivery, such as opening a bank account, SIM card registration, processing or renewing travel documents, or driving licenses, many citizens find themselves denied access to such services.

[22] *State of Internet Freedom in Africa, 2021 https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2021-Report.pdf*

[23] *Compelled Service Provider Assistance for State Surveillance in Africa: Challenges and Policy Options https://cipesa.org/2023/04/compelled-service-provider-assistance-for-state-surveillance-in-africa-challenges-and-policy-options/*

Opportunities

37 of the 55

African countries enacted personal data protection laws

Over the last two decades, the continent has registered tremendous progress in adopting enabling legal frameworks to protect and promote the rights to privacy and personal data protection. With Cape Verde leading the process in 2001, at least 37 countries have now enacted personal data protection laws, with at least 29 countries having followed up with the establishment of data protection authorities.[24] The enactment of personal data protection laws in at least 37 of the 55 African countries presents an excellent opportunity to advance the protection of data subject rights within the context of BDI programmes. This is because it is now easier to hold data processors accountable for data privacy breaches.

Secondly, the coming into force of the African Union Convention on Cyber Security and Personal Data Protection (the "Malabo Convention") in June 2023, after Mauritania became the 15th state to submit its ratification, also boosted the legal landscape. The operationalisation of the Malabo Convention means that all 15 State Parties are obliged to take all the necessary measures to implement the convention at the national level.[25] More specifically, Article 10(4) of the Malabo Convention calls upon states to refrain from processing personal data involving biometric data unless authorised by a relevant protection agency established by law, such as the Data Protection Office. In addition, Article 14(6)(a) of the Malabo Convention prohibits data controllers from transferring personal data to a non-member State of the AU unless such a State ensures an adequate level of protection of the privacy, freedoms, and fundamental rights of persons whose data are being or are likely to be processed. Other AU initiatives, such as the Digital Transformation Strategy for Africa and AfCFTA, have been candid in articulating the importance of ethical processing of biometric digital identities in promoting trust and transparency for Africa's growing digital economy.

The existence of several global initiatives, such as the World Bank's Identification for Development (ID4D) Initiative, that are designed to help practitioners design and implement identification (ID) systems that are inclusive and trusted, offer great opportunities to push and remodel existing and new BDI programmes based on the ten Principles on Identification for Sustainable Development and other international standards and good practices.[26]

[25] *Round up of Data Protection in Africa 2023 - https://assets-global.website-files.com/641a2c1dcea0041f8d407596/660c183b35ce75f5eb7b5654_Roundup%20on%20Data%20Protection%20in%20Africa%20-%202023.pdf*

[26] *Africa: AU's Malabo Convention set to enter force after nine years https://dataprotection.africa/malabo-convention-set-to-enter-force/*

[27] *World Bank Identification for Development Initiative https://id4d.worldbank.org/guide/about-guide*

Policy Options

Given the above initiatives, policies and practices foregoing, there are several policy options that both governments and private entities should adopt to enhance the benefits and mitigate the risks and challenges associated with the ongoing biometric digital identity data collection and processing programmes.

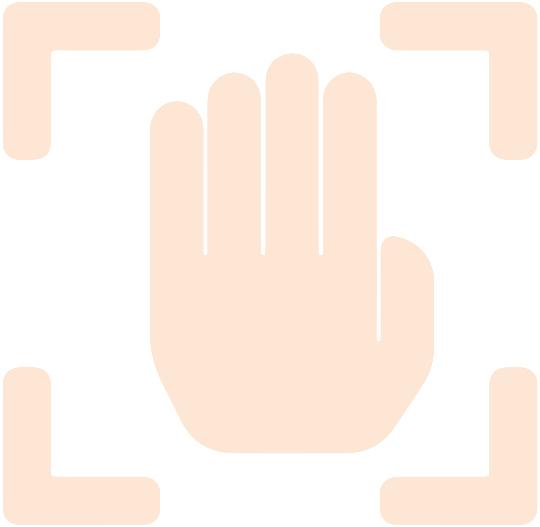
First, countries must be pushed to develop and implement a robust and compliant legal framework for BDI systems, consisting of policies, laws, regulations, and codes of practice across the continent. As discussed above, while 37 countries have standalone data protection laws, only 29 have established and operationalised the relevant data authorities and commissions responsible for implementing and monitoring the progress of the data protection laws. However, the majority of the commissions are dogged by several challenges, including a lack of political and financial independence. While most of these agencies have de jure autonomy bestowed by the laws, they are often expected to report to a minister or member of the executive arm. The laws give line ministers discretionary powers, including the power to revise regulations, grant exemptions, decide on the enforcement of rules, and review penalties, and budget allocations, making regulatory agencies prone to political interference including regulatory capture.[27] For digital rights and justice actors, it is, therefore, vital to push for the amendment of the relevant laws to ensure the financial and political independence of the commissions.

Secondly, existing legal and policy frameworks must be popularised and well-understood by the citizens to appreciate their inherent rights as data subjects and hold data collectors accountable. Without a proper understanding of their rights as data subjects, many data controllers, including government agencies, will continue abusing and derogating citizens' rights to privacy and data protection. Governments should, therefore, collaborate with other key stakeholders such as civil society, the media, and academia to develop and roll out public awareness programmes on privacy and data protection, particularly during the conceptualisation and implementation of each data collection programme.

Thirdly, it is crucial that governments, in partnerships with critical actors such as civil society, academia, and tech companies, undertake comprehensive capacity-building programmes for data collectors and state officials, particularly those responsible for biometric data collection programmes, including data protection bodies, law enforcement, prosecution, regulators, and the judiciary, in the effective protection and promotion of data protection rights. Many data collectors and processors have limited knowledge about data rights and their responsibilities to data subjects, especially in government-driven programmes, most of which are forced onto the citizens with dire consequences of non-compliance, including denial of services if one does not have a relevant ID.

[27] *Assessing Data Protection and Privacy in Africa https://www.jstor.org/stable/pdf/resrep25330.7.pdf?refreqid=-fastly-default%3Abc524caaea493cc41bfe59e4764aad44&ab_segments=&origin=&initiator=&acceptTC=1*

Fourthly, poor infrastructure - especially the poor and intermittent internet connectivity that is driven partly by lack of electricity and other logistical challenges has remained an Achilles in African digitisation endeavours, requiring holistic interventions, including incentives for private internet service providers and telecom companies to spread their reach including to hard to reach places that do not make economic sense and supporting rural electrifications programs throughout the continent. Governments must allocate resources to build a robust digital ecosystem with national geographical coverage.



Suggested citation:
CIPESA (2024) Biometrics and Digital Identity in Africa: Challenges, Opportunities and Policy Options

March **2024**

CIPESA

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