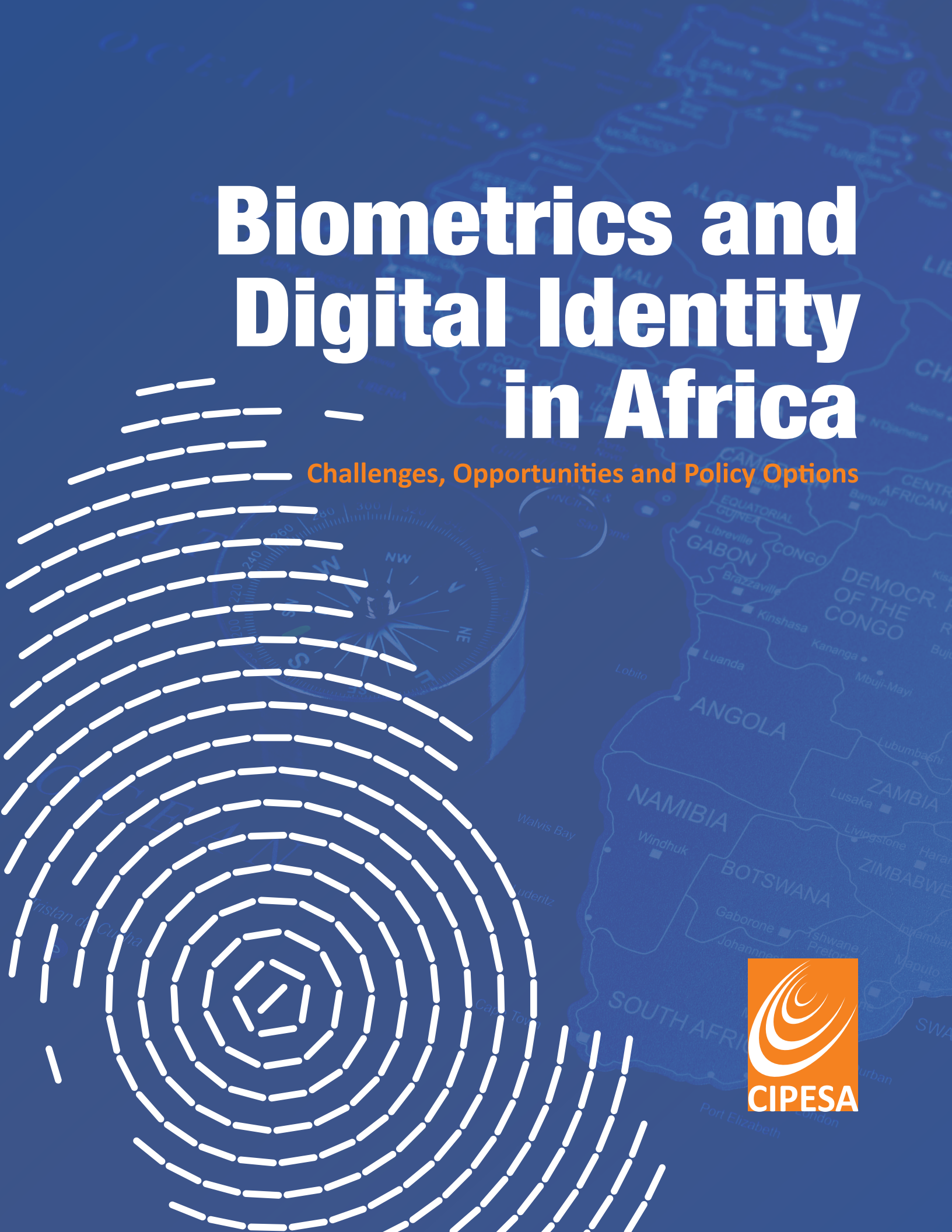
Biometrics and Digital Identity in Africa

Challenges, Opportunities and Policy Options



Introduction

Africa has witnessed an accelerated appetite for collecting and processing citizens' biometrics as countries transition from paper-based to digital identities. Biometrics such as fingerprint, facial, or iris recognition 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 within the African Union's Digital Transformation Strategy for Africa (2020-2023)[1] and the Africa Continental Free Trade Agreement (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. In many countries, however, the enabling legal and policy framework is weak, with some countries lacking specific data protection laws, rendering the protection of the massively harvested and processed personal biometric data insufficient and exposed to risks such as identity theft and unregulated state surveillance, among others.

Although the African Union (AU) has issued several guidelines through instruments such as the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention)[3] and the AU Data Policy Framework[4] calling upon Member States to only engage in the processing of personal data involving biometric data after authorisation by the relevant protection authority and create an enabling legal environment that would achieve and maximize the benefits of a data-driven economy, respectively, challenges still abound. The adoption and implementation of biometric digital identity systems has increasingly become a trend in Africa, spurred by recent technological advancements that have led to accelerated digitization of activities and services, such as e-government, e-identification or digital identification, e-commerce, and digital banking. While the goals for the Biometric Digital IDs (BDIs) 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 policy brief, we discuss some of the critical drivers of BDIs, the challenges, opportunities, and policy options for African countries, and how they can leverage the socioeconomic and political dividends of biometric digital identities 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

Over the last decade, the collection and processing of BDI data has gained traction partly due to emerging technological advancements and the need to digitize government services and operations.

Improving Service Delivery

Governments' appetite has partly been driven by the need to transform service delivery and enhance public participation by developing central databases. Because data has become central to planning and economic transformation, the adoption of biometric data and digital identities has been identified as one way of improving efficiency in service delivery. More specifically, critical government programs that have necessitated the collection and processing of biometrics have included civil registration, such as the issuance of National Identity cards, updating of biometric voter registration and identification programmes, government-led CCTV programmes with facial recognition capabilities, national e-Passport initiatives, refugees' registration, and mandatory biometric SIM card registration, which has driven the demand and adoption of digital ID credentials, both of which are critical to access digital services.[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 several regional initiatives that necessitate collecting and processing biometric digital identities. For example, in July 2016, the African Union (AU) unveiled the continent's first electronic passport to ease movement, with a target of complete adoption by 2020. While this has yet to come to pass, several countries and economic blocs have embraced the concept and introduced e-passports to their citizens, which have electronic chips to store the biometric information 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 ePassport with a target of phasing out the old passports by November 2022. Both the African Union's Data Policy Framework and Digital Transformation Strategy for Africa (2020-2030) provide additional catalysts for countries to embrace digital identities, including creating an enabling legal environment that would achieve and maximize 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*

Recent Technological Advancements

Recent technological advancements have also accelerated the adoption of BDIs as being authentic, secure, and reliable compared to paper-based identifiers, and as technology becomes more accessible and affordable, governments and private entities continue to leverage biometrics and biometric technologies 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 addition, the proliferation and adoption of mobile biometric solutions, including their multifactor authentications (MFA) that enable secure access to services on the go, have accelerated faster ID enrolment and verification, enabling greater inclusion and accessibility to services.[11] 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 biometric identification (e.g., 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.[12] As companies push to digitise their services, the need for biometric authentication has intensified with users' options for online transactions instead of physical interactions. For the majority of the users, effective participation in any digitisation programs involving the processing of their personal data will depend on their perception and confidence that the data is secure and free from misuse.[13]

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 *Obid*

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

13 *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.*

Challenges to BDIs in Africa

In their current state, Biometric Digital Identify programs 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 data protection national laws are not robust enough nor 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 different legal provisions for purposes of processing biometrics such as fingerprints, photos, signatures, and iris scans, for purposes of facilitating SIM card registration, voter registration, and issuance of national identification. The legal framework providing for the protection of personal data has remained insufficient with almost thirty percent of countries needing more specific laws on the protection of personal data. 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,[14] Kenya's Data Protection Act 2019,[15] 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[16] have weak safeguards, including provisions for circumstances under which sensitive information can be accessed, such as safeguarding national security, public interest, enforcement of the law, and conduct of criminal investigations. The existential lack of clarity and precision in the existing personal identity and biometric data laws creates room for ambiguity and misinterpretation.[17]

Secondly, the lack of clarity and precision in laws governing personal identity and biometric data leaves room for ambiguity and misinterpretation. In addition, the prevalence of 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, DRC, Tanzania, and Uganda had their amended almost a decade ago. The lack of a robust data protection legal framework reduces public trust in any data processing programs.[18] The lack of comprehensive legislative and governance structures, such as independent oversight and redress mechanisms, exacerbates the issues of surveillance, data protection concerns, and cybersecurity as they play a critical role in the design, implementation, and operation of digital ID systems, including defining what is and what is not permissible, particularly regarding the processing and sharing of personal data and biometric information, outline ID users' consent, control and rights, define the scope of identity verification and authentication, establish oversight bodies or regulatory authorities.[19]

14 *Article 18*

15 *Part V (section 44-47)*

16 *section 9*

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

18 *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*

19 *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.[20] The assistance rendered by intermediaries facilitates internet disruptions, easy access to users' data, content removals, decryption of users' encrypted data, and state surveillance.[21]

Fourthly, the non-universality and the slow-phased way these programs are implemented has resulted in non-documented citizens, especially in rural or hard-to-reach areas, particularly those with poor internet connectivity due to limited or no access to electricity, with almost 600 million people (accounting for 43%) of the population, in Sub-saharan Africa.[22] 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.

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

21 *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/*

22 *Electricity Access in Sub-saharan Africa https://cleanenergy4africa.org/electricity-access-in-sub-saharan-africa-world-bank-report/*

Opportunities

In 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.[23] The progressive enactment of personal data protection laws in at least 37 of the 55 African countries presents an excellent opportunity to advance the promotion and protection of data subject rights within the context of BDI programs. It is now easier for advocates to hold data processors accountable for breaches of any data subject rights.

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 55 AU member states are required to domestic cyber security, private, and data protection laws within their legal frameworks.[24] 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, Principle 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 African Union's Digital Transformation Strategy for Africa (2020-2023)[25] and the Africa Continental Free Trade Agreement (AfCFTA),[26] 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 programs based on the ten Principles on Identification for Sustainable Development and other international standards and good practices.[27]

23 *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*

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

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

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

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

Policy Options

Given the foregoing, there are several policy options that both governments and private entities must adopt and push for to enhance the benefits and mitigate the risks and challenges associated with the ongoing biometric digital identity data collection and processing programs.

First, countries must be pushed to develop and implement a robust and proportionate legal framework for BDI systems consisting of policies, laws, regulations, and codes of practice across the continent. As discussed above, while 37 countries have comprehensive standalone data protection laws, only 29 have established and operationalised the relevant data authorities and commissions responsible for the implementation and monitoring progress of the data protection laws. However, majority of the commissions are dogged by several challenges, including a lack of political and financial independence. This is because, 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 and regulatory capture. For 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 accountable data collectors. 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 - civil society, the media, academia, etc to develop and roll out public awareness programs on privacy and data protection, particularly during individual data collection programs.

Thirdly, it is crucial that governments, in partnerships with critical actors such as civil society, academia, and tech companies, undertake comprehensive capacity-building programs 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 programs, 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.

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 endeavors, 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.

28 *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*

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