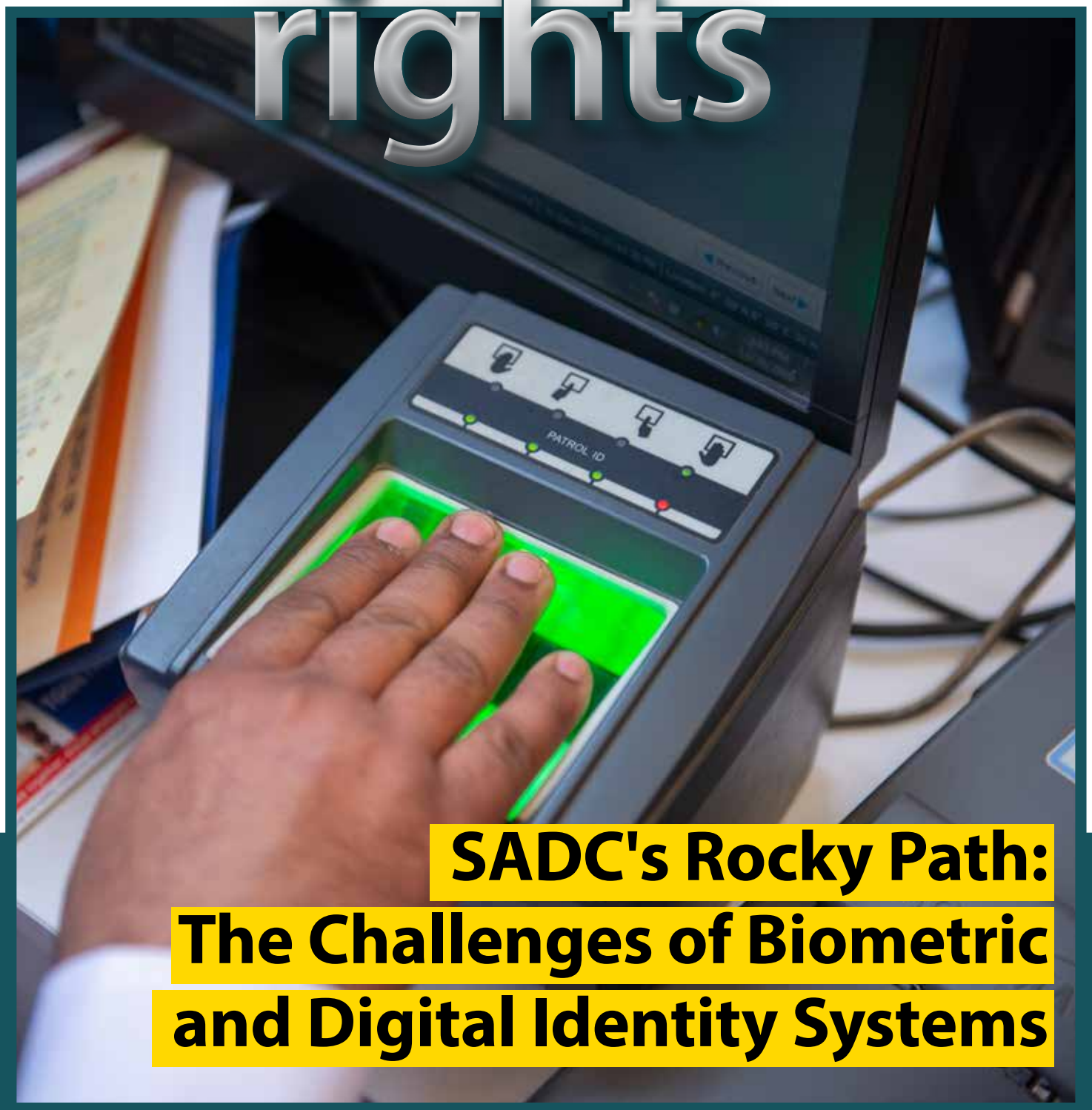
# digital rights SOUTHERN AFRICA

Issue No. 03 April 2024




# SADC's Rocky Path: The Challenges of Biometric and Digital Identity Systems

AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS

# African Declaration on Internet Rights and Freedoms

A fundamental challenge in need of urgent resolution in the digital age is how to protect human rights and freedoms on the Internet, and the African continent is no exception. The African Declaration on Internet Rights and Freedoms was developed in response to this challenge.

## 13 PRINCIPLES:

1. Openness

2. Internet Access and Affordability

3. Freedom of Expression

4. Right to Information

5. Freedom of Assembly and Association and the Internet

6. Cultural and Linguistic Diversity

7. Right to Development and Access to Knowledge

8. Privacy and Personal Data Protection

9. Security, Stability and Resilience of the Internet

10. Marginalised Groups and Groups at Risk

11. Right to Due Process

12. Democratic Multistakeholder Internet Governance

13. Gender Equality

# Contents




digital rights
SOUTHERN AFRICA

**ISSUE 03**

APRIL 2024

**Southern Africa Digital Rights** is produced under 'The African Declaration on Internet Rights and Freedoms: Fostering a human rights-centred approach to privacy, data protection and access to the internet in Southern Africa' project.

**Editorial Board:**
Peace Oliver Amuge (APC)
Zoé Titus (NMT)
Frederico Links (Coordinator)

**Copy editors:**
Reyhana Masters
Lis Jordan

**Layout & production:**
Boldrin Titus

**Cover picture:**
PradeepGaurs, Shutterstock

**Contributors:**
Thapelo Ndlovu (Botswana)
Melusi Matsenjwa (Eswatini)
Jimmy Kainja (Malawi)
Dianne Hubbard (Namibia)
Levy Syanseke (Zambia)
Helen Sithole (Zimbabwe)

**Published and distributed by:**
Association for Progressive Communications (APC)
133, 2nd Avenue, Melville 2092,
Johannesburg, South Africa

Namibia Media Trust (NMT),
13 Adler Street, Windhoek,
Namibia

**Funded by:**
Open Society Initiative for Southern Africa
1st Floor, President Place
1 Hood Ave. / 148 Jan Smuts Ave.
Rosebank, Johannesburg,
South Africa

**Correspondence can be sent to:**
Namibia Media Trust
info@nmt.africa

# Editorial

## Spotlight on the vexing questions around biometrics and digital IDs

FREDERICO LINKS

Across the continent biometric data collection systems are being implemented at an increasing pace and for a variety of reasons. And yet, as this issue of *Digital Rights Southern Africa* makes clear, there is no or slow commensurate roll-out of measures to ensure that such biometric data collection and processing systems are secure and to the actual benefit of the societies in which they are being implemented. Oftentimes the installation of these biometric data collection systems is closely linked to the creation of digital identification (ID) systems.

It its 2022 State of Internet Freedom in Africa report, which focused on the roll-out of biometric data collection systems across the continent, the Collaboration for ICT Policy in East and Southern Africa (CIPESA) found that these systems are meant 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".

However, CIPESA pointed out that these systems "present new risks to the realisation and enjoyment of human rights and freedoms".

Similarly, with respect to digital ID systems, on the recent International Identity Day, which fell on 16 September 2023, global privacy rights advocacy group Privacy International (PI) emphasised that there was a global "identity crisis" because "the technology-driven ID systems being implemented around the world are leading to new forms of surveillance and exclusion".

This is a serious charge, as these systems are touted as being implemented in the interest of personal and societal safety. However, PI found that while there "are numerous reasons given by proponents for the introduction or use of an ID system, including identity fraud prevention, national security, crime prevention, financial industry facilitation and the prevention of human trafficking", these systems are actually being used in many cases "to facilitate targeting, profiling and surveillance".

**Across the continent biometric data collection systems are being implemented at an increasing pace and for a variety of reasons. And yet, as this issue of Digital Rights Southern Africa makes clear, there is no or slow commensurate roll-out of measures to ensure that such biometric data collection and processing systems are secure and to the actual benefit of the societies in which they are being implemented.**

It was against this backdrop that we felt it necessary to place the issues around biometric data collection and processing systems and digital IDs under a glaring regional light.

As this issue illustrates, the "worrying manifestations" of concerns around these systems cut across the six spotlighted countries and the region as a whole.

Eswatini has become the bellwether in terms of violations on the regional digital rights landscape, and in this edition regulatory happenings in that country once again paint a threatening picture.

In Botswana, Namibia and Malawi authorities are struggling to come up with legislative measures to safeguard privacy rights as they seek to craft biometric data collection and digital ID policies, or to implement such systems where frameworks already exist.

In our Zambia contribution there is a call for a citizen-centric approach to implementing such systems, while in Zimbabwe concerns abound about the state's intentions with digital ID systems.

In the end, it remains unclear what impact these systems will have on the countries under the spotlight, but one thing is certain, the trends are worrisome.

With this edition, then, we hope to inform advocacy groups across the region to be on guard as biometric data collection and processing, as well as digital ID, systems are rolled out on them.

We need to be vigilant.

Good reading!

---


Botswana's national ID, Omang.
Photo credit: Weekend Post

# Essential reforms needed **to elevate biometric data protection**

T H A P E L O  N D L O V U

*Botswana's Biometric Data Security Challenges and Urgent Calls for Legal Reforms*

Biometrics involve biological data stored digitally which is unique to individuals. According to the United Nations Children's Fund (UNICEF), biometric technologies utilise measurable physical traits like fingerprints, facial images, and iris scans to identify or verify a person's identity.

Various entities, including banks, e-commerce platforms, civic registration authorities handling birth and death records, mobile service providers for SIM card registration, and agencies issuing identity cards and passports, maintain personal information. These platforms are susceptible to potential breaches by malicious actors seeking to exploit vulnerabilities.

This discussion delves into the vulnerabilities of identification cards, e-passports, SIM cards, and financial institutions that collect biometric data in exchange for services. It explores how the increase in biometric data-related crimes exposes weaknesses in these systems, posing a threat to people's right to privacy.

## The case of Botswana

Botswana is reputed to be the first country in the Southern African Development Community (SADC) to successfully introduce identification cards with the Automated Fingerprint Identification System (AFIS) and according to the United Nations Conference on Trade and Development (UNCTAD) sponsored National ICT Policy Review and E-commerce Strategy for Botswana (2021), "is in the process of upgrading this system to into a single, multi-biometric and multiple-use new-generation platform."[1]

Although the initiation of National Identification cards, locally recognised as Omang ('who are you?'), dates back to 1988, Botswana only ratified the Data Protection law in 2018. This legislative stride was designed to regulate the collection of personal data, ensuring monitoring and governance over its acquisition and storage by both public and private entities (Data Protection Act, 2018). This legal framework aimed to assuage concerns regarding potential misuse of personal information in the era of biometrics, a landscape previously devoid of regulatory oversight[2].

The Legislative Framework Change Report (2004), arising from a benchmarking exercise to formulate Botswana's ICT policy, forewarned of the requisite measures for safeguarding personal data, particularly in light of burgeoning digital biometric technologies[3]. Discussions pertaining to identity theft and the impetus behind the Data Protection Act had been underway.

## Salient Biometric Advancements

There are key biometric developments that have taken place over time which form a picture of the country's status on the matter.

- **Identification Cards**

The crux of Botswana's biometric progression hinges on the Automated Fingerprint Identification System (AFIS), inaugurated in 1988 to preclude duplications. These ID cards incorporate dual-layered security protocols, enabling visual and machine-based readability[4]. Mandated for citizens aged 16 and above, these cards ensure a direct linkage between birth and death registrations (ID4D, 2018).

Omang functions as an elemental document for services necessitating biometric identification. On registration, individuals furnish personal details encompassing name, age, date and place of birth, eye colour, height, and a portrait image captured by the issuing department. All these are visible on the card upon production while some of the information is machine readable.[5]

- **Sim Card Registration**

In 2009, the government of Botswana introduced registration of mobile phones' sim-cards. The Executive Director of the then Botswana Telecommunication Authority (BTA), Thari Pheko was quoted as saying the initiative was meant to fight crime and that it was 'international best practice'.[6]

Since then, when installing a new sim card, registration is required, where upon personal data is provided. At the time the initiative was introduced, the media cried foul, insisting the system was open to abuse as the media has, as some of its stakeholders, undisclosed sources.

The Media Institute of Southern Africa (MISA) was fearful that media sources would be targeted for personal and political reasons (Afrol.com). Also of interest is the requirement to repeat this biometric information whenever a service is required from mobile operators. This means the information is available to all and any customer service personnel handling calls at any given time.

1 UNCTAD https://unctad.org/system/files/official-document/dtlstict2021d4_en.pdf

2 One trust Data Guidance https://www.onetrust.com/products/data-guidance/

3 Maitlamo, Botswana National ICT Policy - Legislative Frame work and change Report2004 https://ictpolicyafrica.org/en/document/khdaorfc689?page=1

4 ID4D, World Bank, 2016) https://www.studocu.com/ph/document/university-of-the-philippines-system/electrical-engineering/botswana-id4d-diagnostic-web-040418/14195549

5 ibid

6 Afrol News http://www.afrol.com/articles/29785

- **e-passport**

Botswana introduced the e-passport in 2010 and this was regarded as a move to curb forgery and other related misdemeanours.[7]

Just like the ID cards, e-passports require retention of biometric information in digital systems, leaving the data subjects with no control over the safety of such information. It is, however, notable that the passports are said to be installed with an Extended Access Point (EAC) in their security chip, which is expected to mitigate illicit access.[8]

## Human Rights Considerations

All the projects identified run short of strict assurance to respect or adhere to human rights. The service users are often not given an option or explanation but are expected to just give away their personal data. The human rights approach in the collection of biometric data is lacking. The whole PANEL concept is breached as there is no participation, accountability, non-discrimination, empowerment and legality in the process. The examples discussed below will demonstrate this observation.

- **Multi-national corporates and data flight**

Data subjects are not in control of their information, especially its retention by the processors. Personal data is often passed around across different jurisdictions with the assumption of prior consent from the customer. While these conglomerates publish privacy statements alerting users of the possible flight of their personal data,[9] customers in need of urgent services would usually just give away their biometrics.

Institutions such as banks maintain distinct privacy policies, often shaped by legislative mandates within their home jurisdiction and not originating in Botswana. Take Stanbic, a subsidiary of the Standard Bank group, for example. It adheres to the same privacy protocols centralised at Standard Bank. Notably, the bank, like others, elucidates its privacy and data stance on its website, outlining its approach and procedures.

However, this scenario underscores the limited influence customers in Botswana wield over the destination of their personal data, a clear human rights concern[10]. This issue is not exclusive to Stanbic or the banking sector; it is widespread among companies with headquarters abroad. For instance, customers of Multichoice might receive calls from individuals in Zambia, promoting the company's offerings and seemingly possessing intimate knowledge of the customer's biometrics. Similarly, insurance companies like Hollard, operating their customer service desks from South Africa, solicit personal data, including biometrics, from customers in Botswana, despite claiming domicile within the country.

Ernst & Young (E&Y) Botswana is another example of an institution who publishes a 'Privacy Statement' on its website, in what appears to be proactively absolving themselves from possible legislative issue in their host jurisdictions. Just like others, E&Y is a global company that shares its customer data across different jurisdictions.[11] Despite the publishing of privacy statement, customers are ignorant of the way their personal information is passed around. Worse still, even if they are aware, they have no option if they want the service provided. It must be noted that all this is contrary to the provisions of the Data Protection Act, 2018, which is explicit in Section 48 (1) that: "the transfer of personal data to other countries is prohibited."[12]

---

7 Sunday Standard, 2010 https://www.sundaystandard.info/botswana-introduces-electronic-passport/#:~:text=Finally%2C%20the%20most%20awaited%20E,readable%20electronic%20passport%20in%20Gaborone.

8 networkweek.net

9 Stanbic Bank privacy statement https://www.stanbicbank.co.bw/botswana/personal/About-us/privacy-and-security-statement

10 ibid

11 Earnst and Young Privacy statement https://www.ey.com/en_bw/privacy-statement

12 Data Protection Act 2018 https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf

- **Identity theft and surveillance**

Mmegi (2020) highlighted a surge in incidents of identity theft in Botswana, particularly during the Covid-19 period. Criminals engaged in phishing tactics to obtain individuals' identities, gaining access to their personal and financial information[13]. They masqueraded as reputable organisations, ostensibly seeking information to aid the targeted individuals. Once they acquired a fragment of information, such as age, these criminals exploited it to acquire further details.

Social media platforms are inundated with narratives of scammers contacting unsuspecting customers of mobile operators, often falsely claiming to offer services or declaring that the customers have won prizes. These calls, appearing authentic and furnished with accurate customer information, coax individuals into confirming banking or mobile money account details. In certain instances, individuals are coerced into depositing money into provided accounts.[14]

The Sunday Standard (2020) reported on Orange Money, a prevalent mobile money service in Botswana, acknowledging awareness of the reported scams through its parent company, Orange.

- **Surveillance**

Botswana has advanced its surveillance ambitions over the years and with the advent of technologies, this has become prevalent. Surveillance is also provided for in law, notably the Intelligence and Security Act, which allows the Director General to secure a court order to intercept private communications.[15]

An illustrative case involved a retired senior soldier, Pius Mokgware who won an out of court case, in which he accused his former employer (Botswana Defence Force) of targeting him for surveillance. It was revealed the surveillance was done through intercepting his phone communications with the assistance of an employee of a state-owned Botswana Telecommunication Corporation's then subsidiary, be Mobile.[16]

Another development related to surveillance has been the installation of street cameras by the Botswana police. The cameras, installed in partnership with Huawei technologies, are said to be fitted with facial recognition technology.[17] This has raised fears that, contrary to what they are officially meant for, which is to fight crime, the use of this technology is vulnerable to abuse. While there has not been a public case specifically arising from the CCTV surveillance, the 'body language' of government justifies suspicions. In January 12, 2022, government gazetted and pushed to parliament a bill seeking a blank cheque to snoop and intercept the public's private communications.[18]

The Criminal Procedures and Evidence (controlled Investigations) Bill 2022 alerted the nation to the government's appetite for surveillance. The push back was successful as it resulted in a watered-down version.[19]

Section 16 (i) of the initial bill gave the head of investigation a right to order interception of communication without a court warrant. Civil society amongst them the Universal Periodic Review Working Group consisting of several NGOs, considered the bill an affront to human rights, and an intrusion into someone's privacy.[20]

---

13 Mmegi, 2020 https://www.mmegi.bw/opinion-analysis/keeping-your-identity-safe-through-a-pandemic/news

14 Sunday standard, 2020 https://www.sundaystandard.info/orange-botswana-warns-of-scammers/#:~:text=The%20fraud%20works%20like%20this,value%20is%20usually%20P4%2C000.

15 State of Internet Freedom in Botswana, 2019

16 Sunday Standard, details of BDF intelligence illegal spying on former deputy commander kept secret, 28 February 2013 https://www.sundaystandard.info/details-of-bdf-intelligence-illegal-spying-on-former-deputy-commander-kept-secret/

17 LONDA- Botswana Digital Rights and Inclusion, 2020 report https://paradigmhq.org/report/londa-digital-rights-and-inclusion-in-botswana/

18 Government Gazette Extraordinary- Criminal Procedures and Evidence (controlled Investigations) Bill January 12, 2022 https://cpj.org/wp-content/uploads/2022/01/Botswana-Criminal-Procedure-and-Evidence-Bill.pdf

19 VOA-Botswana Government waters down phone tapping Bill after public outcry, February 4, 2022 https://www.voanews.com/a/6426756.html

20 UPR Working Group statement, February 1, 2022 https://www.facebook.com/ditshwanelobotswana/posts/upr-ngo-working-group-press-statement-on-the-criminal-procedure-and-evidence-con/2086553018220146/

The bill further provided for interference with the national civil registration database as it allowed for 'assumed identities' to be officially recognised through regular registration and issuance of identity documents. This would have the effect of embellishing the national civic registration with fake biometric information and in the process eroding the integrity of the identity process.

## Legal instruments

International legal instruments that recognise the right to identity and nationality include the Universal Declaration of Human Rights and the Convention on the Rights of the Child, resolution 44/25 of November 20, 1989 (ID4D, World Bank, 2016). There is, however, scanty specific mentions of biometric data protection in many legal instruments, with the General Data Protection Regulation of European member states being one of the few that addresses it specifically.[21]

A number of laws in Botswana facilitate the use of Biometric data and some even speak to its protection. The Cyber Crime and Computer Related Crimes Act of 2007/8 provides the basis to curb digital crimes. The law, as in Section 17, can be helpful in preventing unlawful disclosure of information gained through provision of service.[22] In practice, however, the law has been largely used to frustrate whistle blowing and to protect the reputations of politicians. It has been used, for instance, to arraign people for 'maligning the leadership' thereby limiting their freedom of expression

While the Data Protection Act of 2018 was also expected to protect privacy and personal data, it has not been fully enforced and no public awareness campaigns have been conducted. This is one law, which, while it can do with some improvement, is informed by international best practices. Section 25 (i and ii) of the Act specifically speaks to 'Processing of genetic data and Biometrics.' Another notable mention is Section 48 and 49 that prohibits cross border data flight as discussed above under the multi-national corporates subheading.

**The enforcement of the right to privacy, particularly regarding the protection of biometric data, remains insufficient, both in terms of legal provisions and practical application**

The Children's Act, Section 23 provides for the right to privacy for children. While it can be argued that collection of the child's biometric information is in both the child and public interest, and the confidence that the system is locked against any intrusion, stolen identity is still possible.

## Conclusion

The enforcement of the right to privacy, particularly regarding the protection of biometric data, remains insufficient, both in terms of legal provisions and practical application. While certain laws, such as the Data Protection Act of 2018, make mention of biometric data, there's a pressing need for a dedicated law that comprehensively addresses and elaborates on this critical matter. The current legislation only touches upon biometric data briefly, necessitating a more expansive scope and detailed reflection within the legal framework.

Given the prevalence of identity theft, state surveillance, financial fraud, and other related crimes, treating biometric data as a peripheral concern is no longer viable. Financial institutions tend to merely present privacy statements as a formality, neglecting to implement additional measures that ensure customers fully comprehend the risks associated with divulging their biometric data. Moreover, these institutions are complicit in what can be termed as 'data flight,' wherein personal data is exchanged among their branches globally, sometimes conducting customer interviews via phone from international offices. Such practices persist despite the explicit provisions within the Data Protection Act of 2018 addressing the issue of data flight.

21 Thales Group- Biometric Data and Privacy Laws (GDPB, CCPA/CPRA) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data

22 State of Internet Freedom in Botswana, 2019

Consequently, the conclusion arises that biometric data collection in Botswana lacks the essential components integral to human rights: participation, accountability, non-discrimination, empowerment, and legality.

## Observations and recommendations

- There exists a deficiency in legal frameworks safeguarding personal biometric data. Government should urgently enforce the Data Protection Act in Botswana.
- Government should develop a dedicated Biometric Data Protection Act that comprehensively addresses the rights of diverse segments of society, including children, persons with disabilities, and those living in poverty.
- Civil society displays apathy toward issues concerning biometric data protection, underscoring the necessity for a comprehensive mapping of necessary actions.
- The public and civil society at large should participate in the formulation of laws; hence, the recommendation stands to establish a platform facilitating engagement for civil society organisations and the public before parliamentary debates to either adopt or reject bills.
- Government should prioritise the operationalisation of the Data Protection Act of 2018, and desist from adopting conflicting laws that impact negatively on citizen's right to privacy.

## References


1. UNCTAD https://unctad.org/system/files/official-document/dtlstict2021d4_en.pdf
2. One trust Data Guidance https://www.onetrust.com/products/data-guidance/
3. Maitlamo, Botswana National ICT Policy - Legislative Frame work and change Report 2004 https://ictpolicyafrica.org/en/document/khdaorfc689?page=1
4. ID4D, World Bank, 2016) https://www.studocu.com/ph/document/university-of-the-philippines-system/electrical-engineering/botswana-id4d-diagnostic-web-040418/14195549
5. ibid
6. Afrol News http://www.afrol.com/articles/29785
7. Sunday Standard, 2010 https://www.sundaystandard.info/botswana-introduces-electronic-passport/#:~:text=Finally%2C%20the%20most%20awaited%20E,readable%20electronic%20passport%20in%20Gaborone.
8. networkweek.net
9. Stanbic Bank privacy statement https://www.stanbicbank.co.bw/botswana/personal/About-us/privacy-and-security-statement
10. ibid
11. Earnst and Young Privacy statement https://www.ey.com/en_bw/privacy-statement
12. Data Protection Act 2018 https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf
13. Mmegi, 2020 https://www.mmegi.bw/opinion-analysis/keeping-your-identity-safe-through-a-pandemic/news
14. Sunday standard, 2020 https://www.sundaystandard.info/orange-botswana-warns-of-scammers/#:~:text=The%20fraud%20works%20like%20this,value%20is%20usually%20P4%2C000.
15. State of Internet Freedom in Botswana, 2019; https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Botswana-2019.pdf
16. Sunday Standard, details of BDF intelligence illegal spying on former deputy commander kept secret, 28 February 2013 https://www.sundaystandard.info/details-of-bdf-intelligence-illegal-spying-on-former-deputy-commander-kept-secret/
17. LONDA- Botswana Digital Rights and Inclusion, 2020 report https://paradigmhq.org/report/londa-digital-rights-and-inclusion-in-botswana/
18. Government Gazette Extraordinary- Criminal Procedures and Evidence (controlled Investigations) Bill January 12, 2022 https://cpj.org/wp-content/uploads/2022/01/Botswana-Criminal-Procedure-and-Evidence-Bill.pdf
19. VOA-Botswana Government waters down phone tapping Bill after public outcry, February 4, 2022 https://www.voanews.com/a/6426756.html
20. UPR Working Group statement, February 1, 2022 https://www.facebook.com/ditshwanelobotswana/posts/upr-ngo-working-group-press-statement-on-the-criminal-procedure-and-evidence-con/2086553018220146/
21. Thales Group- Biometric Data and Privacy Laws (GDPB, CCPA/CPRA) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data
22. State of Internet Freedom in Botswana, 2019 https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Botswana-2019.pdf

# Risk of human rights infringement as Eswatini rushes **to regulate the ICT sector**

MELUSI MATSENJWA

*Human rights should not be sacrificed at the altar efficiency and convenience*

The Kingdom of Eswatini has been striving to catch up with its Southern African counterparts in information and communication technology (ICT) development. Until 2017, citizens in this small kingdom had only one mobile phone operator, MTN Eswatini, which had maintained a monopoly in the mobile telephony sector since 1998. The Eswatini Posts and Telecommunications Corporation (EPTC), previously a service provider and regulator, underwent a transformation following the amendment of its establishing act. Subsequently, the regulatory role shifted to the Eswatini Communications Commission (ESCCOM), established in 2013 under the Swaziland Communications Act of 2013[1]. Operating under the Ministry of Information Communication and Technology, this commission oversees all ICT-related laws, including the Swaziland Communications Commission Act of 2013[2], Electronic Communications Act of 2022[3], Electronic Communications Transactions Act of 2022[4], Computer Crime and Cybercrime Act of 2022[5], and the Data Protection Act of 2022[6].

Eswatini is still very much a novice in the area of regulation of the ICT sector. It is within this legal framework that biometrics and digital systems are regulated. Rollout of most these systems, however, started before comprehensive legal and policy frameworks were put in place. These systems are being implemented in SIM card registrations, voter registration and verification, civil registration, financial services accessibility and inclusion.

## SIM card registration

In 2016, exercising the Swaziland Communications Commission Act, the Minister of ICT published Legal Notice No. 26 of 2016. The scope and object of the regulation was to provide a framework for the registration of all mobile subscribers in Swaziland and the protection of the subscriber information collected.[7] Mobile phone operators were enjoined by these regulations to record and store personal information of existing and new subscribers. This information included, among other things, names, addresses, identity numbers, and facial images for natural persons, encompassing both local citizens and non-Swazi individuals.

1 https://www.dataguidance.com/sites/default/files/the_swaziland_communications_commission_act_2013.pdf

2 https://www.esccom.org.sz/legislation/SwazilandCommunicationsCommissionAct.pdf

3 https://www.esccom.org.sz/legislation/SwazilandElectronicCommunicationsAct.pdf

4 https://www.esccom.org.sz/legislation/ELECTRONIC%20COMMUNICATIONS%20TRANSACTIONS%20ACT.pdf

5 https://www.esccom.org.sz/legislation/COMPUTER%20CRIME%20&%20CYBERCRIME%20ACT.pdf

6 https://www.esccom.org.sz/legislation/DATA%20PROTECTION%20ACT.pdf

7 https://www.esccom.org.sz/regulations/The-Electronic-CommunicationsSubscriber-Registration-Regulations2016.pdf

**The Kingdom of Eswatini has been striving to catch up with its Southern African counterparts in information and communication technology (ICT) development.**

According to the Regulation, service providers are required to retain this information for up to five years after the termination of the customer's contract or the conclusion of service by the provider.[8] Additionally, service providers have an obligation under the Regulation to safeguard subscriber information and prevent unauthorized sharing of this data.

## Biometric voter registration

In 2013, during the national elections, the Elections and Boundaries Commission (EBC), which is the elections management body in the Kingdom, for the first time, used a Biometric Voter Registration System for the registration of voters. This enabled the EBC to capture photo and fingerprint biometrics of each voter.[9] This same system was also used in the 2018 elections.

## National identification card

In 2003, the Kingdom initiated the National Identification Card, which includes the owner's facial identity, full names, date of birth, chief code, and Personal Identity Number (PIN), among other details. This information is centrally stored by the Ministry of Home Affairs. However, despite recent developments allowing service providers like commercial banks to access the civil registry for identity verification, the National ID card does not yet meet the criteria for digital identification. For instance, the facial identity alone does not grant direct access to the PIN or other vital details such as a physical address, and vice versa. This significant biometric disparity highlights that the current form of the national ID is not fully exploitable in line with its potential.

Expanding the scope of the ID card system to encompass broader digital identification could yield both benefits and complications. Enhancements in digital identification might streamline access to services and online transactions, offering convenience. However, this expansion also raises privacy and security concerns, as consolidating extensive personal information in one system could attract malicious attempts to access or misuse such data. Hence, the consideration involves striking a balance between convenience and safeguarding personal information.

## More time needed for stakeholder input

A quick scan of the local environment shows that the national government has not started rolling out digital identity in earnest even though there have been significant efforts at putting in place the legislative framework as can be seen in the enactment of the four pieces of legislation in 2022. The legislative process is such that ordinarily, stakeholders and members of the public have an opportunity to make inputs when the law is at Bill stage. The time for that is shortened significantly as the bills were tabled with a certificate of urgency. All four Acts mentioned above were tabled before Parliament with certificates of urgency.

8 Regulation 10(2) page 18 https://www.esccom.org.sz/regulations/The-Electronic-CommunicationsSubscriber-Registration-Regulations2016.pdf

9 https://www.idea.int/answer/ans738857696091

Photo credit: Shutterstock

Given their technical nature, it would be expected that they would only attract industry players in the ICT space but even they did not have the sufficient time to make their inputs. There are indications, however, that through the Royal Science and Technology Park (RSTP), initiatives are being conceptualised in this regard and could be rolled out in the not-so-distant future.

## Strategies for ICT development

Developments in the area of biometrics and digital identity find expression in the country's national development strategies on ICT. For instance, the National Information and Communication Infrastructure (NICI) Implementation Plan is aligned with the NICI Policy Vision. This vision aims to utilise ICT infrastructure and solutions to shape a modern Twenty-First Century Kingdom of Eswatini, fostering sustainable socio-economic development, accelerated poverty reduction, and equal opportunities regardless of gender or physical ability. The plan outlines goals across various Priority Areas: Human Resource Capacity, Infrastructure Development, Education, Strategic ICT Leadership, Financial Services Sector, ICT Industry, Legal/Regulatory Frameworks, Environmental Management, and Media. [10]

Another strategy would be the National Cybersecurity Strategy 2022-2027, one of whose goals is to foster a safe and secure information society for Eswatini.[11] The African Union's (AU's) *Digital Transformation Strategy* sees digital IDs as one of the main cross-cutting areas to support the digital ecosystem and as a key mechanism for promoting the UN concept of 'legal identity for all' and attaining sustainable development goals (SDGs) and Agenda 2063.

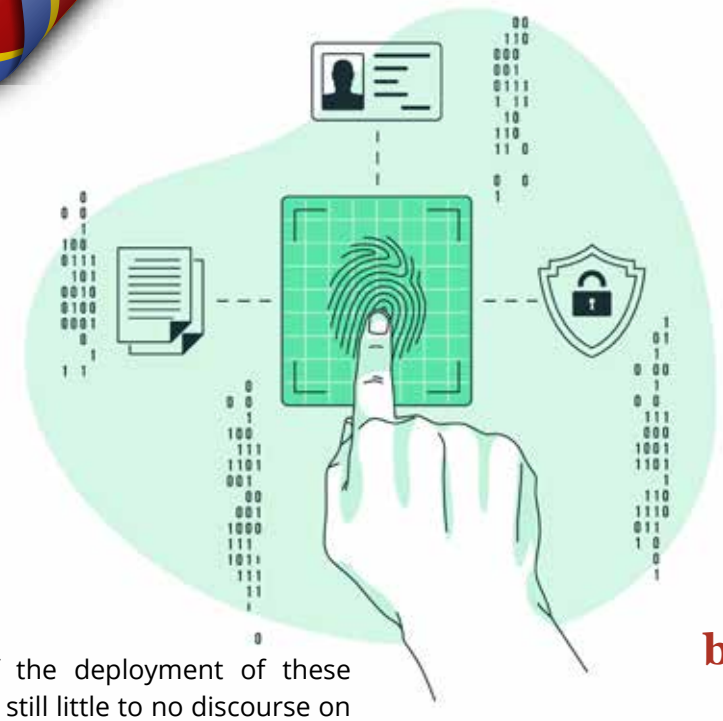
## Possible benefits of biometric and digital identification systems

Nothing much is available where government is making a case or justification for deployment of biometric and digital identification systems, however, sectoral interests, particularly the banking sector see huge benefits for the industry as this will form a good basis for Electronic Know Your Customer (e-KYC). For emerging economies like Eswatini, digital identity is seen as capable of unlocking value of up to 6 per cent of the Gross Domestic Product (GDP). This can happen in the following ways:

- Digital ID can improve the efficiency of labour markets as it streamlines verification processes, enhances mobility, reduces paperwork, allows for efficient onboarding and offers better tracking and analysis: high unemployment rate in Eswatini, particularly among the youth.
- Digital ID can boost the productivity of land and agriculture through formalized land ownership: Swazi Nation Land (tribal land) vs Title Deed Land.
- Digital ID can increase access to financial services (financial inclusion).[12]
- Digital ID can help government gain revenue through the elimination of ghost workers and social security consolidation which could facilitate a more seamless process in Government to Person Payments (G2P)

Other sectors that would benefit from the full deployment of these systems are the revenue collection authority and security and law-enforcement.

10 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Eswatini%20NCS%202020.pdf
11 https://www.gov.sz/images/ICTDOCUMENTS/Eswatini-National-Cybersecurity-Strategy-2022-2027.pdf
12 https://digitalfrontiersinstitute.org/wp-content/uploads/2020/11/DID-Week-2020-Final-Summary-16-11-2020.pdf



## Conclusion

Given the infancy level of the deployment of these systems in Eswatini, there is still little to no discourse on these issues. As with most technical pieces of legislation, debates usually start once enforcement begins and the full effect of the law is laid bare. Passing the laws on an urgent basis contributed immensely to the absence of consultation and public debate. If the experiences of most African countries who are deploying these systems at full throttle is to be referenced, threats to such freedoms as association and expression are real, especially given that politically, a lot remains tentative in the country given the tensions. It does not help that the Kingdom generally does not have a good human rights record.

Although these advancements could offer significant societal benefits, it's crucial for civil society to remain vigilant and well-informed about their potential impact on human rights. Civil society needs to continuously monitor legislative and policy reform and learn from peers from the region and beyond. It must continue contesting the space for consultation, put in place robust advocacy strategies that are informed and raise public awareness. Human rights should not be sacrificed the altar of efficiency. In a context of already shrinking civil society space, there is need to guard against further curtailment of the enjoyment of rights. In addition to the regional, continental and international human rights obligations, Eswatini is enjoined to protect the constitutionally guaranteed rights to freedom of expression, to privacy, expression and association, among others.[13]

**Passing the laws on an urgent basis contributed immensely to the absence of consultation and public debate.**

### References


1. https://www.dataguidance.com/sites/default/files/the_swaziland_communications_commission_act_2013.pdf
2. https://www.esccom.org.sz/legislation/SwazilandCommunicationsCommissionAct.pdf
3. https://www.esccom.org.sz/legislation/SwazilandElectronicCommunicationsAct.pdf
4. https://www.esccom.org.sz/legislation/ELECTRONIC%20COMMUNICATIONS%20TRANSACTIONS%20ACT.pdf
5. https://www.esccom.org.sz/legislation/COMPUTER%20CRIME%20&%20CYBERCRIME%20ACT.pdf
6. https://www.esccom.org.sz/legislation/DATA%20PROTECTION%20ACT.pdf
7. https://www.esccom.org.sz/regulations/The-Electronic-CommunicationsSubscriber-Registration-Regulations2016.pdf
8. Regulation 10(2), page 18: https://www.esccom.org.sz/regulations/The-Electronic-CommunicationsSubscriber-Registration-Regulations2016.pdf
9. https://www.idea.int/answer/ans738857696091
10. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Eswatini%20NCS%202020.pdf
11. https://www.gov.sz/images/ICTDOCUMENTS/Eswatini-National-Cybersecurity-Strategy-2022-2027.pdf
12. https://digitalfrontiersinstitute.org/wp-content/uploads/2020/11/DID-Week-2020-Final-Summary-16-11-2020.pdf
13. Swaziland Constitution Act 1 of 2005


13 Swaziland Constitution Act 1 of 2005

# Malawi dragging its feet on **filling legal gaps to prevent human rights violations**

JIMMY KAINJA

*Malawi's Data Initiatives - Balancing Progress and Privacy Concerns*

In July 2022, Malawi's state president inaugurated the country's first data centre in its commercial city, Blantyre. This initiative resulted from a partnership between the Government of Malawi and the Chinese technology company Huawei. It builds upon previous data collection programmes, starting with the biometric national ID registration in 2017 and the mandatory SIM card legislation in 2018.

The government has provided several justifications for these programmes, emphasising their benefits. They have been largely met with acceptance, evidenced by the minimal resistance from civil society organisations within the country and the compliance demonstrated by Malawians. However, it is essential to consider potential implications; some argue that these initiatives might have adverse effects on human rights, particularly digital rights, due to their potential role in enabling surveillance.

## Data centre

In July 2022, Malawi became the latest African country to commission a National Data Centre in partnership with the Chinese company Huawei. Huawei has partnered with other African countries, including Zambia, Uganda, South Africa, Mozambique and Senegal.

These partnerships are part of Huawei's drive to expand its African data centre programmes. The company's Vice President of Public Affairs and Communications told Africa News that his company is a "partner to build the data centre, to provide the equipment, the platform and to improve the connection with the applications of the different partners.[1]" Malawi President, Lazarus Chakwera, believes that the National Data Centre is a "positive step into the country's digital future." He holds the view that they would guarantee the "security of information" and thus attract investors in the "manufacturing, financial, retail, and service sectors.[2]"

There is no reason to doubt the president's commitment to his statements and his genuine intentions for the country. Undoubtedly, the fourth industrial revolution demands that nations embrace emerging digital technologies, including big data. However, such investments necessitate concurrent commitments to robust data security, including the establishment of comprehensive data protection laws, a facet currently absent in Malawi's governance.

Moreover, the lack of public access to the terms of the Malawi Government's collaboration with Huawei, raises pertinent questions about access to information within the National Data Centre. This concern holds merit, especially considering Huawei's contentious track record in data centre projects.

1 João Marques Lima (2021), Huawei Lines Up for Africa Data Centre Expansion. Available at: https://thetechcapital.com/huawei-lines-up-for-africa-data-center-expansion/ (accessed 20 March 2023)

2 Regtech Africa (2022), Malawi: Malawi Opens First National Data Centre in Blantyre. Available at: https://regtechafrica.com/malawi-malawi-opens-first-national-data-centre-in-blantyre/ (accessed 20 March 2022)

Notably, in 2019, an investigation by *The Wall Street Journal*[3] revealed instances where Huawei employees, embedded within cybersecurity forces in Uganda and Zambia, intercepted encrypted communications and utilised call data to monitor political opposition. Despite Huawei's denial of involvement, their persistent investment in data centres prompts scrutiny.

The dismissal of *The Wall Street Journal's* report as Western media in certain circles reflects the geopolitical tensions between the West and China. This tension arises from allegations asserting Huawei's cybersecurity risks in the USA and the UK. However, despite such dismissal, the report prompts crucial inquiries about the potential misuse of these infrastructures by the state for citizen surveillance and potential human rights violations.

Notably, there have been numerous instances in Malawi where individuals faced detention and arrest over WhatsApp conversations and journalists were targeted for their professional work[4] . These incidents serve as indicators of the state's inclination towards monitoring its citizens. Therefore, any technology facilitating surveillance would likely find acceptance in such a context.

## National ID registration

In 2017, the Government of Malawi launched the biometric national ID registration, mandating registration for all citizens aged 16 years and older. The National Registration Bureau (NRB), as stipulated by the National Registration Act of 2010, holds the responsibility to execute, coordinate, manage, and sustain Malawi's National Registration and Identification System (NRIS)[5].

Norman Fulatira, the NRB's spokesperson, highlighted in *The Nation* (2021) newspaper that Malawi trailed behind other Southern African nations in implementing citizen registration and issuing national identity cards. Fulatira asserted that the nation's status as the last in the region to roll out national ID cards has been advantageous for Malawians, who have now been issued smart cards[6] . The NRB asserts that the primary objective of the national ID is to ensure "positive identification of every individual in the country."

Additionally, according to the NRB, the national ID enhances both national and international security by facilitating the "easier traceability of foreigners. [7]"

The programme received substantial participation, registering nine (9) million people within the initial six months. Since its implementation, the national ID has replaced previously separate ID systems, including passports, driving licenses, and voter registration cards. All government entities now require the national ID for services such as passport issuance, driver's license acquisition, tax number registration, SIM card registration, voter registration, accessing agricultural subsidies, and participating in cash transfer programmes. Banks mandate customers to undergo a 'Know-Your-Customer' process, necessitating the presentation of their national ID.

The National Democratic Institute (NDI)[8] observes that digital ID systems offer convenience but raises concerns regarding control over information collection, data storage, and utilisation, which pose significant challenges for democracy. NDI further contends that centralised ID systems could potentially be exploited to intimidate specific communities, perpetuate existing inequalities, and discriminate against marginalized groups historically excluded from exercising their civic and political rights.

---

3 Joe Parkinson, Nicholas Bariyo and Josh Chin (2019) Huawei Technicians Helped African Govenments Spy on Political Opponents. Available at: https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

4 Jimmy Kainja (2022), Arrests Mar Malawi's Digital Rights Landscape. Available at: https://www.apc.org/en/news/arrests-mar-malawis-digital-rights-landscape (accessed 20 March 2023)

5 National Registration Bureau. Available at: https://www.nrb.gov.mw/index.php (accessed 20 March 2023)

6 Norman Fulatira (2021), Why do National IDs Expire? Available at: https://mwnation.com/why-do-national-ids-expire/#:~:text=%E2%80%9CCommon%20sense%E2%80%9D%20is%20another%20reason,features%20such%20as%20facial%20image. (accessed 20 March 2023)

7 NRB, National IDs, a Solution to Malawi's Problems. Available at: https://www.google.com/search?q=purpose+of+national+id+-card+malawi&oq=purpose+of+national+id+card+malawi&aqs=-chrome..69i57j33i160.14427j0j4&sourceid=chrome&ie=UTF-8 (accessed 20 March 2023)

8 Priyal Bhatt, Sarah Moulton and Elizabeth Sutterlin (2021), Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalised Communities. Available at: https://www.ndi.org/sites/default/files/Identified%20but%20Unheard%20FINAL.pdf (accessed 20 March 2023)

## Mandatory SIM card registration

In 2018, the Government of Malawi enforced mandatory SIM card registration, as outlined in section 92(1) of Communications Act No. 34 of 2016[9] . This regulation mandates that any user of a generic number or possessor of a SIM card for voice telephony services must "register that generic number or SIM card with any electronic communications licensee or with the distributor, agent, or dealer authorised by the electronic communications licensee to provide or sell generic numbers or SIM cards."

Section 92(1)(a) stipulates that subscribers must provide the following details: (i) their full name; (ii) identity card number or any other document that proves the identity of the subscriber; and (iii) residential and business or registered physical address of the subscriber.

The policyholder, Malawi's telecommunications regulator, the Malawi Communications Regulatory Authority (MACRA), stated that the SIM card registration would help achieve the following[10]:

- Prevent SIM boxing[11].
- Help recover stolen phones.
- Protect subscribers from hate texts, threats and incitation of violence.
- Create a conducive environment for all phone users and instil discipline in those abusing phones.
- Help law enforcers track down criminals who use phones for illegal activities.
- Curb fraud and theft that occurs through the use of phones.

Hence, SIM card registration purportedly aimed to safeguard subscribers from criminal activities and facilitate the identification of offenders. This rationale gained the trust of Malawian citizens, resulting in the implementation encountering minimal public opposition. However, the implementation of SIM card registration occurred in the absence of robust data protection legislation and adequate legal safeguards to shield subscribers from potential data misuse, considering that mobile phone users in the country can no longer maintain anonymity. Furthermore, the SIM card is directly linked to the national ID.

While the Malawi Communications Regulatory Authority (MACRA) has enumerated various accepted forms of identification for SIM registration, it is apparent that all licensed agents responsible for registering SIM cards mandate a national ID for the registration process[12].

Privacy International warns that SIM card registration can facilitate surveillance and having their private information misused. It can also facilitate discrimination and exclusion of those unable to register SIM cards because they do not have identification. Malawi's national ID has an expiry date[13], and there are increased cases where national ID cards take months to be renewed upon expiration.

While the introduction of SIM card registration in Malawi proceeded without significant resistance or adequate legislation to safeguard subscribers, evidence indicates that this measure has not effectively curbed crime in the country. In February 2023, MACRA disclosed that cybercriminals siphon approximately $117,000 monthly in Malawi, a concerning statistic considering that 10.1 million out of 17.5 million Malawians possess a mobile wallet[14].

---

9 The Malawi Gazette (2016), *Communications Act, No. 34 of 2016.* Government Press

10 MACRA, Why is it Important to Register SIM Card? Available at: https://macra.mw/frequently-asked-questions-2/ (accessed 20 March 2023)

11 What is SIM Boxing? Available at: https://www.dignited.com/44776/what-is-sim-boxing/ (accessed 20 March 2023)

12 MACRA, What are the Acceptable Documents? Available at: https://macra.mw/frequently-asked-questions-2/ (accessed 20 March 2023)

13 Norman Fulatira (2021), Why do National IDs Expire? Available at: https://mwnation.com/why-do-national-ids-expire/#:~:text=%E2%80%9CCommon%20sense%E2%80%9D%20is%20another%20reason,features%20such%20as%20facial%20image. (accessed 20 March 2023)

14 Johnstone Kpilaakaa (2023), In Malawi, Mobile Money Users Get Scammed of About $117K Monthly. Available at: https://www.benjamindada.com/malawi-mobile-money-wallet-fraud/ (accessed 20 March 2023)

Despite the clear security implications, there exists no collaboration between MACRA and security agencies to mitigate this fraud, underscoring the need for increased capacity within the police force[15].

Efforts have been discussed to foster collaboration among the police, MACRA, and bolster security agencies; however, no tangible steps have been taken. These systemic inefficiencies imply that mandatory SIM card registration has fallen short in curbing fraudulent activities. If anything, incidents of mobile money-related crimes have risen post-SIM card registration. Privacy International observed that despite accumulating evidence highlighting the costly and intrusive nature of mandatory SIM registration, many governments persist in implementing it annually, despite its inefficacy in addressing the underlying issues they aim to solve[16].

## Conclusion and implications

Implementing the National Data Centre, the biometric national ID registration and the mandatory SIM card registration means that the Malawi Government has assembled a robust data collection and centralisation programme within five years. Malawians' acceptance of these programmes implies that people willingly surrender their data without knowing how it will be handled, who has access to it and for what purposes. Although privacy is provided for under section 21 of the Malawi Constitution, Malawi lacks robust data protection law to actualise section 21, which provides that "every person shall have the right to personal privacy, which shall include the right not to be subject to a) searches of his or her person, home or property; b) the seizure of private possessions; or c) interference with private communications, including mail and all forms of telecommunications".

The Data Protection and Privacy Bill 2021 remains in its draft form. However, the Bill indicates that the government is aware of the need for a robust data protection law, especially in the digital era.

The draft Bill's memorandum states that "as the Malawi economy becomes increasingly reliant on digital technologies, there is a need to protect personal data of individuals collected, generated, stored and utilised by public and private sector institutions including in the provision of healthcare, health and other types of insurance, education, banking and financial services, hospitality services, civil registration, voting, immigration, national ID and delivery of social programmes[17]".

As reported by *TechTarget,* data protection is the process of safeguarding important information from corruption, compromise or loss. The report observes that "the importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates". This captures the essence of the data centralisation programmes' problem without data protection law. The mass collection and centralisation of personal data without legal guidelines make people vulnerable to human rights abuses, particularly surveillance. Surveillance undermines human and digital rights, including privacy, freedom of speech, association, assembly, thought, and protection of citizens' reputations. Glen Greenwald noticed: "People radically change their behaviour when they know they are being watched. They will strive to do that which is expected of them. ... They do so by adhering tightly to accepted social practices, staying within imposed boundaries, avoiding actions that might be seen as deviant or abnormal.[18]"

Thus, the Government of Malawi ought to enact the data protection bill to fill the legal gap and prevent possible human rights violations. Furthermore, civil society organisations should proactively monitor government initiatives that could jeopardise digital rights, rather than reacting only after policies and legislation are in place.

15 Duncan Mlanjira (2022), MACRA to Establish Digital Forensic Lab with Malawi Police to Counter Mobile Money Fraud. Available at: https://www.nyasatimes.com/macra-to-establish-digital-forensic-lab-with-malawi-police-to-counter-mobile-money-fraud/ (accessed 4 April 2023)

16 SIM Card Registration: The Mandatory Registration and Identification of all Mobile Phone Users Purchasing a pre-paid SIM card. Available at: https://privacyinternational.org/learn/sim-card-registration (accessed 20 March 2023)

17 Paul Crocetti, Stacey Peterson, and Kim Hefner, What id Data Protection and Why is it Important ? Available at: https://www.techtarget.com/searchdatabackup/definition/data-protection (accessed 20 March 2023)

18 Glen Greenwald (2014), The Harm of Surveillance. Available at: https://policyoptions.irpp.org/magazines/old-politics-new-politics/greenwald/ (accessed 20 March 2023)

## References


1. João Marques Lima (2021), Huawei Lines Up for Africa Data Centre Expansion. Available at: https://thetechcapital.com/huawei-lines-up-for-africa-data-center-expansion/ (accessed 20 March 2023)
2. Regtech Africa (2022), Malawi: Malawi Opens First National Data Centre in Blantyre. Available at: https://regtechafrica.com/malawi-malawi-opens-first-national-data-centre-in-blantyre/ (accessed 20 March 2022)
3. Joe Parkinson, Nicholas Bariyo and Josh Chin (2019) Huawei Technicians Helped African Governments Spy on Political Opponents. Available at: https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017
4. Jimmy Kainja (2022), Arrests Mar Malawi's Digital Rights Landscape. Available at: https://www.apc.org/en/news/arrests-mar-malawis-digital-rights-landscape (accessed 20 March 2023)
5. National Registration Bureau. Available at: https://www.nrb.gov.mw/index.php (accessed 20 March 2023)
6. Norman Fulatira (2021), Why do National IDs Expire? Available at: https://mwnation.com/why-do-national-ids-expire/#:~:text=%E2%80%9CCommon%20sense%E2%80%9D%20is%20another%20reason,features%20such%20as%20facial%20image. (accessed 20 March 2023)
7. NRB, National IDs, a Solution to Malawi's Problems. Available at: https://www.google.com/search?q=purpose+of+national+id+card+malawi&oq=purpose+of+national+id+card+malawi&aqs=chrome..69i57j33i160.14427j0j4&sourceid=chrome&ie=UTF-8 (accessed 20 March 2023)
8. Priyal Bhatt, Sarah Moulton and Elizabeth Sutterlin (2021), Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalised Communities. Available at: https://www.ndi.org/sites/default/files/Identified%20but%20Unheard%20FINAL.pdf (accessed 20 March 2023)
9. The Malawi Gazette (2016), Communications Act, No. 34 of 2016. Government Press
10. MACRA, Why is it Important to Register SIM Card? Available at: https://macra.mw/frequently-asked-questions-2/ (accessed 20 March 2023)
11. What is SIM Boxing? Available at: https://www.dignited.com/44776/what-is-sim-boxing/ (accessed 20 March 2023)
12. MACRA, What are the Acceptable Documents? Available at: https://macra.mw/frequently-asked-questions-2/ (accessed 20 March 2023)
13. Norman Fulatira (2021), Why do National IDs Expire? Available at: https://mwnation.com/why-do-national-ids-expire/#:~:text=%E2%80%9CCommon%20sense%E2%80%9D%20is%20another%20reason,features%20such%20as%20facial%20image. (accessed 20 March 2023)
14. Johnstone Kpilaakaa (2023), In Malawi, Mobile Money Users Get Scammed of About $117K Monthly. Available at: https://www.benjamindada.com/malawi-mobile-money-wallet-fraud/ (accessed 20 March 2023)
15. Duncan Mlanjira (2022), MACRA to Establish Digital Forensic Lab with Malawi Police to Counter Mobile Money Fraud. Available at: https://www.nyasatimes.com/macra-to-establish-digital-forensic-lab-with-malawi-police-to-counter-mobile-money-fraud/ (accessed 4 April 2023)
16. SIM Card Registration: The Mandatory Registration and Identification of all Mobile Phone Users Purchasing a pre-paid SIM card. Available at: https://privacyinternational.org/learn/sim-card-registration (accessed 20 March 2023)
17. Paul Crocetti, Stacey Peterson, and Kim Hefner, What id Data Protection and Why is it Important ? Available at: https://www.techtarget.com/searchdatabackup/definition/data-protection (accessed 20 March 2023)
18. Glen Greenwald (2014), The Harm of Surveillance. Available at: https://policyoptions.irpp.org/magazines/old-politics-new-politics/greenwald/ (accessed 20 March 2023)

# Namibia navigates **biometric data privacy pending civil registration bill**

DIANNE HUBBARD

*Navigating Biometric Data: Namibia's Regulatory Journey and the Urgent Call for Data Protection Safeguards*

Biometrics are being collected for various purposes in Namibia mostly without legal authorisation protection. However, the forthcoming Civil Registration and Identification Bill is expected to lead the way in providing data protection safeguards for personal data including biometrics, while the Data Protection Bill that is in the works will hopefully expand data protection safeguards.

## Civil registration and identification

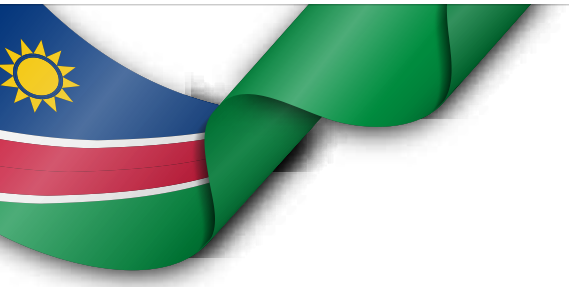
Namibia is in the midst of overhauling its civil registration and identity management systems through the Civil Registration and Identification Bill which is expected to make its way through Parliament in 2023.[1] Many aspects of the new approach contained in this Bill are already in place in practice.

The key innovation in the new system is to link e-notices of birth and death with the identity management system. When a birth takes place in a hospital, medical personnel send an electronic e-notice of the birth to the Ministry of Home Affairs, Immigration, Safety and Security.

One or both parents then apply for birth registration, which has been made more convenient by the provision of registration points at health facilities. The e-notice provides reliable verification that the birth in question took place, and provides information for follow-up if no parent comes forward to complete the registration process.


The Namibian, Twitter post reporting on government announcement, 18 November 2021

1 The author served as a technical adviser to the Ministry of Home Affairs, Immigration, Safety and Security during the development of this Bill.



The proposed law also makes provision for birth registration in respect of children born outside a health facility, abandoned or orphaned children, and for late birth registration of persons of any age. A unique identifying number is assigned to each individual at the time of birth registration.

Deaths are similarly verified by means of an e-notice issued by a health facility or a mortuary, to ensure that death registrations can be confirmed through links to clear physical evidence of the death. Reliable death registration, although often neglected in discussions of civil registration, is vital in the maintenance of a reliable identification database.

Against this backdrop, most people resident in Namibia are required to apply for an identity document upon reaching the minimum age – currently age 16 but set to drop to age 14. Under the proposed law, this duty would apply to citizens, permanent residents, non-citizens with legal authority to be present in Namibia for longer than one year, refugees and other categories of persons that may be identified in future by the Minister – with the colour of the ID card currently indicating the category in question.

The biometrics currently required for the issue of an identification card are a photograph, fingerprints of all ten fingers and any other biometrics that may be set out in future by regulation.[2] For persons whose births were registered in Namibia, the identification number on the ID card will be either the unique identifier assigned at the time of birth registration, or another unique number linked via a confidential system to the birth identifier. Older IDs had a representation of a fingerprint and a bar code on the back, but since 2020, the prescribed format contains a QR code and a machine-readable zone (as illustrated).[3]

Identity documents are generally welcomed in Namibia as the means to facilitate access to education, state welfare benefits and financial services, as well as providing a basis for exercising rights (such as the right to vote) and providing access to a host of other public and private transactions.


Namibia Daily News, "Botswana and Namibia launch National ID Cards as travel documents at port of entry/exit", 24 February 2023

In terms of an agreement between Namibia and Botswana, Namibia's new-style ID cards are recognised as travel documents for citizens moving between the two countries – with this approach expected to spread to other SADC borders.[4] A spokesperson for Amnesty International recently welcomed this move, pointing out that it will reduce barriers to migration and provide an economic boost to informal cross-border traders, especially women – thereby contributing to the alleviation of poverty and food security.[5]

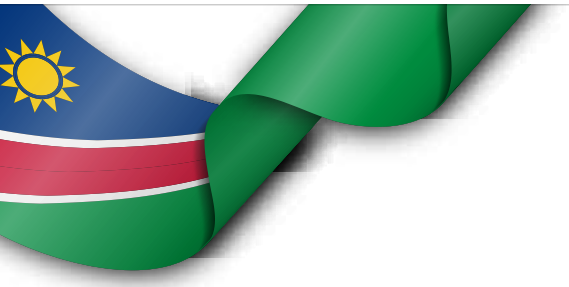
---

2 "Biometrics underpin the uniqueness of identity and bind identities to specific identity holders. Proof of identity is key to maintaining a robust national population register and upholding data integrity. This also ensures that documents such as birth and death certificates, identity cards, and passport and travel documents are trustworthy. In turn, population data integrity means that linked functional registers are accurate." "Case Study 4: Namibia" in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems, *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, Ottawa: International Development Research Centre, 2019, page 103.

3 Identification Regulations, 2001, as amended (issued under the current Identification Act 21 of 1996, which will be replaced in due course by the Civil Registration and Identification Bill.

4 Namibia Daily News, "Botswana and Namibia launch National ID Cards as travel documents at port of entry/exit", 24 February 2023; Gerhard Erasmus & Trudi Hartzenberg, "Botswana and Namibia concluded an agreement on the movement of persons", Tralac, 8 March 2023.

5 "Botswana/Namibia: Accord on free movement between countries a 'step in the right direction'", Amnesty International, 24 February 2023, quoting Tigere Chagutah, Amnesty International's Director for East and Southern Africa.



## Data protection safeguards in the Civil Registration and Identification Bill

The Bill incorporates key data protection principles, which is particularly important given that it is expected to reach Parliament well ahead of the draft Data Protection Bill that is under development.

Access to information in the Ministry's database is strictly regulated by the Bill, although individuals will have a clear right to access information about themselves and to motivate corrections where necessary. There are clear duties of confidentiality with respect to personal data, and access to the database by staff members can be monitored by means of a digital trail.

Data-sharing with other organs of state or with private entities will take place only in terms of memorandums of agreement, and key information regarding such agreements must be published. Law enforcement agencies seeking access to information in the database must use the normal legal procedures that govern searches in other contexts – with the sole exception of accessing fingerprints or other biometric data for the purpose of identifying the body of a deceased person. Access by various intelligence agencies must similarly follow the legal procedures in the laws governing those agencies, which typically require a warrant or other judicial authorization.

Any person will be entitled to reasonable information regarding the security of the database (although only to an extent that will not compromise that security), and the Ministry will be required to maintain an access register that records instances of information-sharing.

## Other instances of biometric data collection and use

In 2018, Namibia's Ministry of Home Affairs introduced a new e-Passport with an electronic microprocessor chip containing biometric information that can be used to authenticate the identity of the passport holder, in order to comply with International Civil Aviation Organization requirements.[6]

Furthermore, Namibia is in the process of rolling out an


Namibia invests in world-class border management, Thales Group, undated

Integrated Border Management System, in which scans of travellers' faces and digital fingerprints are checked against various international watch lists such as lists of wanted criminals, missing persons and lost or stolen travel documents. The data collected at the border is held in a central database hosted by the Ministry. [7] Although such systems at international borders are not unusual, some analysts have expressed concern about possible compromises to the confidentiality of the data in the Namibian system due to the cross-linking across different systems, as well as concerns about the possible ramifications of government dependence on private operators for system function and maintenance.[8]

Other Namibian government agencies also routinely

6 Stephen Mayhew, "Namibia makes the switch to biometric passports", *Biometrics News*, 8 January 2018; Case Study 4: Namibia" in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems, *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, Ottawa: International Development Research Centre, 2019, page 102.

7 "Namibia invests in world-class border management", Thales Group [the company providing the border technology to Namibia], undated. The system has been in place at Hosea Kutako International Airport in Windhoek, since September 2017 and will eventually be extended to all of the country's land, sea, and air borders.

8 Carolina Polito & Dr Cristina Alaimo, "The Politics of Biometric Technologies: Borders control and the making of data citizens in Africa", European Conference on Information Systems (ECIS), Research-in-Progress Papers 78, 2023.

9 Electoral Act 5 of 2014, section 30.

10 Regulations relating to Registration of Voters, Political Parties or Organisations, 2015, regulation 5(2).

11 "Frequently-asked questions", Electoral Commission of Namibia website, accessed 11 May 2023; see also *Namibia Presidential and National Assembly Elections*, Report of the Commonwealth Observer Group, 27 November 2019, pages 17-18.


New and improved Namibian Driver's licence card launched, One Africa, 3 February 2022

collect biometric data. One example is the procedure for voter registration under the Electoral Act. This law requires potential voters to provide a digital image and digital fingerprints[9] - even though many prospective voters will present their Namibian identification card, which is already linked to a fingerprint database. The voter registration card displays a barcode with encrypted registration details, including the voter's name, surname and address along with information on which elections the voter is qualified for (with local and regional elections requiring proof of residency in the relevant constituency or local authority).[10] An electronic "Voters' Registration Kit" at the polling place uses a digital fingerprint scanner to verify the voter's fingerprints against the fingerprints on the electronic voters' roll and produces a record that the voter has voted in the election in question. There is also provision for manual verification if necessary, such as where the barcode is damaged in some way and cannot be scanned.[11]

The process of obtaining a Namibian driving licence also requires a digital image and digital fingerprints (with a manual option in case the driving testing centre does not have the requisite equipment).[12] The driving licence contains a barcode on the reverse side that captures information about the driver, which is linked to an automated biometric system to ensure that the licence is collected by the person to whom it is issued.[13]

Another biometric data collection point is the procedure for applying for Certificates of Conduct from the Namibian Police which provide information on past criminal convictions. These are required for many purposes in Namibia, including tender bids and many job applications. The application procedure involves the taking of digital fingerprints for comparison against the police database, in an effort to ensure that the information provided is accurate.[14] The fingerprints that are collected for this purpose are saved and stored by the Namibian Police, despite the lack of any underlying law governing this process.[15]

Biometric verification is also used in connection with several social grants - either through fingerprint verification against the recipient's Namibian ID, or in the case of benefits provided to veterans of the liberation struggle and their dependants, by means of a separate registration card that includes a photograph, fingerprint and registration number.[16]

Another example concerns the recently-introduced requirements for SIM card registration in Namibia's Communications Act, which requires telecommunications service providers to collect and retain certain information about their customers.[17]


Election Watch, Institute for Public Policy Research (IPPR), Issue No. 9, 2014

12 Road Traffic and Transport Regulations, 2001.

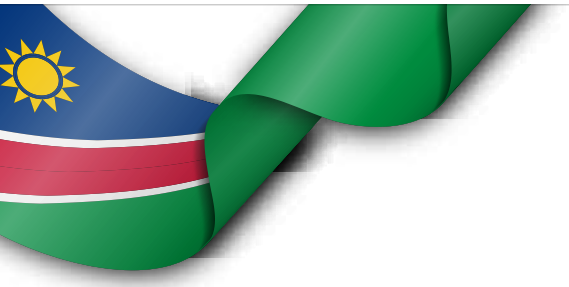
13 See "New Driving Licences Are Here", *Erongo News*, 11 February 2022, quoting Minister of Works and Transport, John Mutorwa.

14 See the discussion of police clearance certificates in "A Sex Offender Register For Namibia? Right Idea, Wrong Solution", Legal Assistance Centre, Pro Bono series, 2022.

15 Personal communication, Criminal Records Office, Namibian Police, May 2023.

16 Veterans Act 2 of 2008, sections 27-ff; Regulations relating to Registration and Benefits of Veterans and Dependants of Veterans, 2008, regulation 6.

17 Communications Act 8 of 2009, section 73: Duty to obtain information relating to customers.



The current regulations require service providers to collect a customer's full name, address and Namibian identity number (which can be substituted by some other form of identification if necessary). The service provider is required to store this information in a manner that allows for retrieval via the customer's name.[18] Service providers are required to store information about the source, destination, date, time and duration of all their customers' telecommunications along with other data - but not including the content of the communication - for at least five years. The Namibian Police or the Namibia Central Intelligence Service can access the stored information with authority from a judge or a magistrate.[19]

The Communications Act makes no mention of biometric collection, but this SIM card registration process is being combined with "voluntary" biometric collection by Namibia's biggest cell provider, MTC - a company in which the government is a majority shareholder.[20] MTC is promoting a digital ID with biometric verification called "Verifi" which was initially presented as an optional way to enhance customer convenience in transactions with MTC, such as SIM cards when a phone is stolen or damaged.[21] In January 2023, MTC announced that the biometrically-supported Verify tool would henceforth be a requirement for accessing any MTC services. assuring customers that this would also cover the requirements of the government-mandated SIM registration.[22] The company promises that the biometrics collected will not be shared without the express consent of the customer, but there is no legal framework as yet to back up this assurance.[23]

This is just one instance of private sector collection of biometrics. Other Namibian companies, including medical aid schemes and financial entities, also collect biometrics.[24] While the consumer in theory has the option to choose another company if there are objections to this approach, Namibia's small economy and thin competition will in many instances make the idea of free choice on this point nothing more than an illusion.

**The improved civil registration and identity management system is envisaged as a foundational system that can ultimately eliminate the need for overlapping biometric data collection and storage by multiple government agencies.**

## Namibia's Data Protection Bill

The widespread increase in biometric data collection and storage makes it urgent for Namibia to enact a strong data protection law. Although a draft has been circulated for discussion, much work is still needed before it will be ready to move forward. The Bill covers the basic international principles on the protection of personal data, but needs strengthening and refinement. The draft currently on the table places restrictions on the processing of biometric and genetic data, but the proposed exceptions need to be carefully considered. [25]

18 Regulations in terms of Part 6 of Chapter V of the Communications Act, 2021, regulation 7.

19 Id, regulations 3 and 5.

20 Until 2021, MTC was wholly owned by a government entity (Namibia Post and Telecommunications Holdings Limited). *MTC Company Profile 2021-2022*, "Who We Are" (unpaginated). The company was listed on the Namibian Stock Exchange in 2021, with a minority of its shares being offered for sale. See, for example, "Govt to raise N$3bn from MTC listing", *The Brief*, 31 July 2021; Ogone Tlhage, "NPTH Undecided Over Unsold MTC Shares", *Namibian Sun*, 8 July 2022.

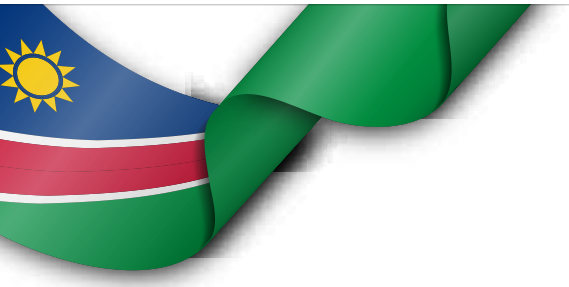
21 "MTC Press Release: MTC Introduces Biometrics And Artificial Intelligence To Protect Consumer Data", 12 January 2021.

22 "MTC Press Release: MTC Verifi KYC Tool in relation to SIM Registration", 31 January 2023.

23 Ibid.

24 For instance, some medical aid providers provide member identification cards that encode digital fingerprints.

25 See "Thinking about data protection" and "LAC submission on the draft data protection bill" in *Perspectives on Parliament,* Issue No. 17, Institute for Public Policy Research (IPPR), December 2022.



## The way forward

There has been little public concern or debate about the collection or security of biometric data. On the one hand, a verifiable identity system is a lynchpin of the government's goal of increasing e-government services – which has the capacity, in the best scenario, of increasing access to government in Namibia's far-flung rural areas.[26]

The improved civil registration and identity management system is envisaged as a foundational system that can ultimately eliminate the need for overlapping biometric data collection and storage by multiple government agencies. The countervailing concern is the need to make sure that inter-operative databases are secure, and that compromised data cannot reveal a multiplicity of information about an individual if encoded linkages to the underlying ID number are penetrated.[27]

The wording of the Namibian Constitution's privacy provision is somewhat narrow. focussing on the right to privacy in respect of "homes, correspondence or communications" – and thus arguably does not cover the collection of biometric data.[28] However, the broader privacy provisions of the *International Covenant on Civil and Political Rights*[29] are incorporated into Namibian law by virtue of Article 144 of the Namibian Constitution which makes international agreements binding upon Namibia part of the law of Namibia.[30] Namibia has also ratified the 2014 *African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention)* – which has not yet garnered sufficient support to come into force[31]. Namibia is in the process of crafting a Cybercrime Bill.[32]

In September 2022, representatives of civil society met to discuss a "Namibian Digital Rights Declaration" which sets out some key principles aimed at ensuring that digital spaces respect and enable rights and serve the public, including vulnerable and marginalised groups. One of the provisions in the draft demands that "privacy and the protection of personal information on- and offline must be urgently prioritised and rights-based safeguards must be enacted in legislation".[33]

Biometric information collection is widespread in Namibia across various contexts, yet public attention towards privacy remains relatively subdued. The issue might only attract significant prominence if an information leak occurs, causing alarm. It is crucial that the Data Protection Bill is not eclipsed by any potential damaging data breaches and progresses swiftly to safeguard against such risks. ■

---

26 See Namibia's e-Government Strategic Action Plan of the Public Service of Namibia (2014-2018).

Alletto Shikololo, "Home affairs embraces e-governance…online passports, work visa applications launched", *New Era*, 16 March 2023. The Electronic Transactions Act 4 of 2019, which provides for the legal recognition of electronic transactions, also helps set the stage for increased e-government.

27 See, for example, "Case Study 4: Namibia" in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems, *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, Ottawa: International Development Research Centre, 2019, page 105; Stephanus van Staden, "Moving the Namibia Civil Registration and Identity System towards an Unified and Federated Service Oriented Population and Identity Management Platform", 2017.

28 Namibian Constitution, Article 13: Privacy. Article 13(1) states: "No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.

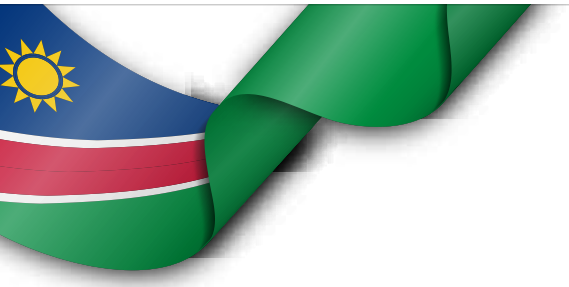
29 *International Covenant on Civil and Political Rights, 1966*, Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

30 Namibian Constitution, Article 144: International Law.

31 *African Union Convention on Cyber Security and Personal Data Protection, 2014*. The AU reported 14 ratifications as of 11 April 2023; see the status list here.

32 See Frederico Links, "Familiar Flaws - Unpacking Namibia's Cybercrime Bill", Institute for Public Policy Research (IPPR), March 2022.

33 See "HAVE YOUR SAY! Draft Namibian Digital Rights Declaration open for public input", Action Coalition website, 4 October 2022.



## References


1. The author served as a technical adviser to the Ministry of Home Affairs, Immigration, Safety and Security during the development of this Bill.
2. "Biometrics underpin the uniqueness of identity and bind identities to specific identity holders. Proof of identity is key to maintaining a robust national population register and upholding data integrity. This also ensures that documents such as birth and death certificates, identity cards, and passport and travel documents are trustworthy. In turn, population data integrity means that linked functional registers are accurate." "Case Study 4: Namibia" in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems, *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, Ottawa: International Development Research Centre, 2019, page 103.
3. Identification Regulations, 2001, as amended (issued under the current Identification Act 21 of 1996, which will be replaced in due course by the Civil Registration and Identification Bill.
4. Namibia Daily News, "Botswana and Namibia launch National ID Cards as travel documents at port of entry/exit", 24 February 2023; Gerhard Erasmus & Trudi Hartzenberg, "Botswana and Namibia concluded an agreement on the movement of persons", Tralac, 8 March 2023.
5. "Botswana/Namibia: Accord on free movement between countries a 'step in the right direction'", Amnesty International, 24 February 2023, quoting Tigere Chagutah, Amnesty International's Director for East and Southern Africa.
6. Stephen Mayhew, "Namibia makes the switch to biometric passports", *Biometrics News*, 8 January 2018; Case Study 4: Namibia" in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems, *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, Ottawa: International Development Research Centre, 2019, page 102.
7. "Namibia invests in world-class border management", Thales Group [the company providing the border technology to Namibia], undated. The system has been in place at Hosea Kutako International Airport in Windhoek, since September 2017 and will eventually be extended to all of the country's land, sea, and air borders.
8. Carolina Polito & Dr Cristina Alaimo, "The Politics of Biometric Technologies: Borders control and the making of data citizens in Africa", European Conference on Information Systems (ECIS), Research-in-Progress Papers 78, 2023.
9. Electoral Act 5 of 2014, section 30.
10. Regulations relating to Registration of Voters, Political Parties or Organisations, 2015, regulation 5(2).
11. "Frequently-asked questions", Electoral Commission of Namibia website, accessed 11 May 2023; see also *Namibia Presidential and National Assembly Elections*, Report of the Commonwealth Observer Group, 27 November 2019, pages 17-18.
12. Road Traffic and Transport Regulations, 2001.
13. See "New Driving Licences Are Here", *Erongo News*, 11 February 2022, quoting Minister of Works and Transport, John Mutorwa.
14. See the discussion of police clearance certificates in "A Sex Offender Register For Namibia? Right Idea, Wrong Solution", Legal Assistance Centre, Pro Bono series, 2022.
15. Personal communication, Criminal Records Office, Namibian Police, May 2023.
16. Veterans Act 2 of 2008, sections 27-ff; Regulations relating to Registration and Benefits of Veterans and Dependants of Veterans, 2008, regulation 6.
17. Communications Act 8 of 2009, section 73: Duty to obtain information relating to customers.
18. Regulations in terms of Part 6 of Chapter V of the Communications Act, 2021, regulation 7.
19. Id, regulations 3 and 5.
20. Until 2021, MTC was wholly owned by a government entity (Namibia Post and Telecommunications Holdings Limited). *MTC Company Profile 2021-2022*, "Who We Are" (unpaginated). The company was listed on the Namibian Stock Exchange in 2021, with a minority of its shares being offered for sale. See, for example, "Govt to raise N$3bn from MTC listing", *The Brief*, 31 July 2021; Ogone Tlhage, "NPTH Undecided Over Unsold MTC Shares", *Namibian Sun*, 8 July 2022.
21. MTC Press Release: MTC Introduces Biometrics And Artificial Intelligence To Protect Consumer Data", 12 January 2021.
22. "MTC Press Release: MTC Verifi KYC Tool in relation to SIM Registration", 31 January 2023.
23. Ibid.
24. For instance, some medical aid providers provide member identification cards that encode digital fingerprints.
25. "Thinking about data protection" and "LAC submission on the draft data protection bill" in *Perspectives on Parliament,* Issue No. 17, Institute for Public Policy Research (IPPR), December 2022.
26. e-Government Strategic Action Plan of the Public Service of Namibia (2014-2018). Alletto Shikololo, "Home affairs embraces e-governance...online passports, work visa applications launched", *New Era*, 16 March 2023. The Electronic Transactions Act 4 of 2019, which provides for the legal recognition of electronic transactions, also helps set the stage for increased e-government.
27. "Case Study 4: Namibia" in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems, *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, Ottawa: International Development Research Centre, 2019, page 105; Stephanus van Staden, "Moving the Namibia Civil Registration and Identity System towards an Unified and Federated Service Oriented Population and Identity Management Platform", 2017.
28. Namibian Constitution, Article 13: Privacy. Article 13(1) states: "No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.
29. *International Covenant on Civil and Political Rights, 1966*, Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."
30. Namibian Constitution, Article 144: International Law.
31. *African Union Convention on Cyber Security and Personal Data Protection, 2014*. The AU reported 14 ratifications as of 11 April 2023; see the status list here.
32. Frederico Links, "Familiar Flaws - Unpacking Namibia's Cybercrime Bill", Institute for Public Policy Research (IPPR), March 2022.
33. "HAVE YOUR SAY! Draft Namibian Digital Rights Declaration open for public input", Action Coalition website, 4 October 2022.

Photo credit: Shutterstock

# Biometric ID rollout should **foreground citizen-centric data protection and privacy**

LEVY SYANSEKE

*Threats to national security and citizens' rights as well as insufficient internet access are concerns*

With a low internet penetration rate, the implementation of the biometric-enabled National ID is a failed project in Zambia.

Zambia, like several Southern African nations, retains 75 percent of its records in physical form, posing challenges in preserving comprehensive citizen histories. This reliance on physical files complicates profiling citizens for various purposes, including security and access to public services. Delays in digitization initiatives persist due to the absence of a biometric-enabled National ID[1].

Discussions advocating for record digitisation, including biometric data collection and digital ID issuance, evoke mixed responses among the populace.

It can be argued that the collection of biometrics in providing digital IDs is for surveillance purposes, this is somewhat true, however, there are other underlying factors. As far back as 2008, efforts to have digital records for citizens in a bid to improve service delivery started. The delay in its execution came about due to the cost of deploying and implementing such a system [2].

1 Terms of Reference Communications Consultant: Development of a Communications Strategy of the INRIS.
Biometric Identity Project – 2019 - https://www.fsdzambia.org/wp-content/uploads/2020/03/ToRs-INRIS-Communications-Strategy-1.pdf

2 Terms of Reference Communications Consultant: Development of a Communications Strategy of the INRIS
Biometric Identity Project – 2019 - https://www.fsdzambia.org/wp-content/uploads/2020/03/ToRs-INRIS-Communications-Strategy-1.pdf

Home Affairs and Internal Security Minister Jack Mwiimbu. Photo: Zambia Monitor

In March 2022, Home Affairs and Internal Security Minister Jack Mwiimbu admitted that the manual system failed to respond to demands arising from the continued growth of the population and rapid changes in technology. This caused issues like duplication of national registration card numbers, identity fraud, and challenges in record management [3].

For instance, replacing a national ID takes at least 30 days if the replacement request is done at a different office from the initial giving office. The explanation for this is, the verification process has to be made and a search in physical records should be done to avoid duplication.

During his update to parliament, the minister informed the country that the development of an - Integrated National Registration Information System (INRIS) had been completed, hardware connectivity set up and the system had been successfully deployed in ten districts across the country.

*"Since then, the manual and paper-based system has not changed despite it being susceptible to fraud and other abuses. The manual-based system lacks the mechanisms to prevent foreigners from registering as Zambians, especially in border areas. Registration officers depend solely on affidavits to register a person. The INRIS, however, will assign a national identity number at birth as opposed to when a person is 16 years old. This will make it very difficult for an ineligible person to register as a Zambian citizen."*[4]

Predominantly, the INRIS is speculated to have been put in place for SIM card registrations, voter registration, and verification and civil registration among others.

Mr. Mwiimbu highlighted the benefits of the digital system including[5]:

a. enhanced security system through proper identification of citizens. Individuals will not easily change their identity as the case may be for some re-offenders;
b. the biometric identification system will contribute towards the promotion of good governance and reduce the cost of voter registration;
c. the Government will minimize wasteful expenditure as ministries, provinces, and other spending agencies will not need to invest in similar biometric identification infrastructure but ride on the INRIS platform;
d. optimization of administration of various Public Service systems such as strengthened tax administration by broadening the tax base, strengthened social services administration by preventing double-dipping and ineligible beneficiaries, and promotion of health insurance administration by providing a unique identity for beneficiaries; and
e. the biometric system will enable digital National Registration Cards (NRCs) with financial wallets, which will contribute towards financial inclusion amongst those individuals or households that do not have an account or relationship with a formal financial institution

3 NANCY SIAME, Parliament K1bn biometric ID issuance starts – 11th March 23 - http://www.daily-mail.co.zm/k1bn-biometric-id-issuance-starts/

4 National Assembly Thursday, 10th March 2022. https://www.parliament.gov.zm/node/10065#:~:text=The%20ministry%20started%20the%20registration,still%20getting%20the%20old%20passports.

5 Lusaka Times – 15th March - 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/

## State justifications for the deployment of the systems

From the government standpoint, improved service delivery by the government required a transition from the old filing system (physical files) to an e-governance system leading to the establishment of the Smart Zambia Office. As such, Biometric Citizen identification is intended to enhance the security system of the country through proper identification of citizens culminating in improved service delivery, identity verification, and significant savings in social cash transfers, Farmer Input Support Program (FISP), Support to Women Livelihood (SWL), pension benefits, and other such social protection programs[6] [7].

A number of government services for the people, such as FISP and Social Cash Transfer, have seen registrations by citizens ineligible to receive them. This is mainly due to duplication, as well as fraud, on the premise of a lack of individualized digital records.

Additionally, in 2019, then minister of Home Affairs,

Former Minister of Home Affairs, Stephen Kapyongo. Photo: ZNBC

Stephen Kapyongo explained that biometric citizen identification had the potential to enhance compliance and therefore contribute towards increased domestic tax revenue mobilization by about 9.5 percent of GDP in the medium term[8].

## Legal underpinnings

The collection of biometrics and issuance of digital IDs is backed by the recently enacted Data Protection Act of 2021 [9] the Cyber Security and Cyber Crimes Act of 2021 [10] and the Electronic Communication and Transactions Act of 2021 [11].

The Ministry of Home Affairs and Internal Security is mandated as the custodian of civil registration under the Department of National Registration Passport and Citizenship (DNRPC) to register all citizens and non-citizens in Zambia. The Ministry draws its mandate from various pieces of legislation, among them, are the Constitution Cap 1 of, the National Registration Act Cap 126 [12], the Passport Act 28 of 2016, the Births and Deaths Registration Act Cap 51, and the Citizenship Act 33 of 2016 of the laws of Zambia [13].

Despite this legislation, the engagement of a foreign company to host the system and have access to national data becomes a threat to national security [14].

6 Michael Malakata March 16, 2022 - Zambia implements biometric ID registration system. https://itweb.africa/content/nWJadMbeW5r7bjO1

7 Digital Identity Country Profile: Zambia - 2019 GSM Association

8 Digital Identity Country Profile: Zambia - 2019 GSM Association

9 https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf

10 https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%204%20of%202021%2C%20The%20Electronic%20Communications%20and%20Transactions_0.pdf

11 The National Registration Act Chapter 126 of the Laws Of Zambia enables the issuance of National Registration Cards (NRCs): https://www.parliament.gov.zm/sites/default/files/documents/acts/National%20Registration%20Act.pdf

12 Ministerial Statement on Implementation of the Integrated National Registration Information System on 10th March, 2022

13 Huawei built data centres that are being run by a quasi-government wing, Infratel. Thus, Government data related to e-governance is being hosted by a quasi-government institution, Infratel.

14 RTSA Reveals Hidden Security and Speed Cameras Mounted in Lusaka by Lensesview - https://lensesview.com/rtsa-reveals-hidden-security-and-speed-cameras-mounted-in-lusaka/?amp=1

**Predominantly, the INRIS is speculated to have been put in place for SIM card registrations, voter registration, and verification and civil registration among others.**

In 2008 in the early phase of developing the system, the government engaged a German-based company that specialised in biometric systems. Giving access to citizen data of such value to a third party is a national security issue and a breach of privacy similar to the case involving the Road Transport and Safety Agency's (RTSA) implementation of speed cameras [15].

With a lack of publicity on the collection of biometrics and issuance of digital IDs for citizens, public reactions have not yet surfaced. However, a few civil society organizations involved in digital rights raised concerns about the increased mounting of surveillance cameras in public spaces without laws or policies backing it up. The concern was not addressed by the government and remained unanswered.

In a young democracy like Zambia, the government needs to get more input from its citizens on such technological advancements. This becomes of concern if national data regarding citizen biometrics and life records are being shared with a foreign company[16] when the local capacity to develop and deploy such systems can be developed. Without the consent of the public to have their biometrics stored by such entities, it becomes a clear breach of data protection and privacy but also a threat to national security.

While biometrics promise enhanced service delivery, the potential for increased citizen surveillance overshadows its efficiency, posing a concern that sufficient legislation is not in place to protect citizens' information. This is based on the premise that the deployment of security cameras in most parts of the country started before the law supported it [17] [18].

Other than the available physical hardware and software necessary for storing such files, the capacity to manage the civil registration system has to be built over time. Additionally, the current slightly above 28% internet penetration rate across the country makes it almost impossible to implement[19] In the case of speed cameras, greater internet penetration can significantly enhance their efficacy, efficiency, and seamless integration into broader traffic management frameworks.

The expected advantages are unlikely to materialise soon due to inconsistent connectivity in most regions. Only if the government prioritises digitising records, improves nationwide internet access, and encourages widespread technology adoption among citizens, will these benefits become feasible. Also, media and civil society must collaborate to raise awareness and advocate for citizen-centric data protection and privacy in the deployment of this system.

In conclusion, the collection of biometrics and issuance of digital IDs in a tech-developing country is critical. Digitisation of records and collection of biometrics is necessary for improved public service delivery. However, before celebrating its deployment, questions regarding the capacity to manage and maintain the system safely should be asked. Questions on connectivity, access, and availability of supporting technology for a woman and child in a remote part of the country for example, should also be addressed. ■

15. RTSA Reveals Hidden Security and Speed Cameras Mounted in Lusaka by Lensesview - https://lensesview.com/rtsa-reveals-hidden-security-and-speed-cameras-mounted-in-lusaka/?amp=1
16 Speed Camera Installation by RTSA a Scandal – UPPZ - August 2018 - https://zambianeye.com/speed-camera-installation-by-rtsa-a-scandal-uppz/
17 Zambia presses ahead with controversial US$210m CCTV camera project by Micheal Malakata – August, 2022 - https://itweb.africa/content/RgeVDMPRY1bvKJN3
18 City Cameras Not Backed by Law, Not Working Yet – Minister – February 9, 2023 - https://zambianobserver.com/city-cameras-not-backed-by-law-not-working-yet-minister/
19 Digital 2022: Zambia - https://datareportal.com/reports/digital-2022-zambia#:~:text=Zambia's%20internet%20penetration%20rate%20stood,percent)%20between%202021%20and%202022.

## References


1. Terms of Reference Communications Consultant: Development of a Communications Strategy of the INRIS
2. Biometric Identity Project – 2019 - https://www.fsdzambia.org/wp-content/uploads/2020/03/ToRs-INRIS-Communications-Strategy-1.pdf
3. Terms of Reference Communications Consultant: Development of a Communications Strategy of the INRIS
4. Biometric Identity Project – 2019 - https://www.fsdzambia.org/wp-content/uploads/2020/03/ToRs-INRIS-Communications-Strategy-1.pdf
5. NANCY SIAME, Parliament K1bn biometric ID issuance starts – 11th March 23 - http://www.daily-mail.co.zm/k1bn-biometric-id-issuance-starts/
6. Michael Malakata March 16, 2022 - Zambia implements biometric ID registration system. https://itweb.africa/content/nWJadMbeW5r7bjO1
7. Digital Identity Country Profile: Zambia - 2019 GSM Association
8. Digital Identity Country Profile: Zambia - 2019 GSM Association
9. https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf
10. https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf
11. https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%204%20of%202021%2C%20The%20Electronic%20Communications%20and%20Transactions_0.pdf
12. The National Registration Act Chapter 126 of the Laws Of Zambia enables the issuance of National Registration Cards (NRCs): https://www.parliament.gov.zm/sites/default/files/documents/acts/National%20Registration%20Act.pdf
13. Ministerial Statement on Implementation of the Integrated National Registration Information System on 10th March, 2022
14. Huawei built data centres that are being run by a quasi-government wing, Infratel. Thus, Government data related to e-governance is being hosted by a quasi-government institution, Infratel.
15. RTSA Reveals Hidden Security and Speed Cameras Mounted in Lusaka by Lensesview - https://lensesview.com/rtsa-reveals-hidden-security-and-speed-cameras-mounted-in-lusaka/?amp=1
16. Speed Camera Installation by RTSA a Scandal – UPPZ - August 2018 - https://zambianeye.com/speed-camera-installation-by-rtsa-a-scandal-uppz/
17. Zambia presses ahead with controversial US$210m CCTV camera project by Micheal Malakata – August, 2022 - https://itweb.africa/content/RgeVDMPRY1bvKJN3
18. City Cameras Not Backed by Law, Not Working Yet – Minister – February 9, 2023 - https://zambianobserver.com/city-cameras-not-backed-by-law-not-working-yet-minister/
19. Digital 2022: Zambia - https://datareportal.com/reports/digital-2022-zambia#:~:text=Zambia's%20internet%20penetration%20rate%20stood,percent)%20between%202021%20and%202022.

Photo credit: Shutterstock. AI was used to generate this image.

# Zimbabwe grapples with **complex realms of biometric and digital identification**

HELEN SITHOLE

*Balancing Benefits and Privacy Concerns in Zimbabwe's Biometric Identity Systems*

The General Data Protection Regulation (GDPR) defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data."[1]

In simpler terms, biometric data refers to any information that can be used to identify an individual based on their unique physical or behavioural characteristics. Examples of biometric data include fingerprints, facial recognition[2], iris scans, voiceprints, and DNA profiles. Biometric identity therefore, refers to identity systems which make use of a set of biometric features to verify an individual's identity.

Under the GDPR and national laws such as Zimbabwe's Cyber and Data Protection Act [3], biometric data is considered a special category of personal data, which means that it is subject to additional protection and restrictions on processing.

1 General Data Protection Regulation: https://gdpr-info.eu/

2 Facial recognition is a form of biometric technology that uses software algorithms to analyse and recognise unique facial features from an individual's image or video.

3 https://www.veritaszim.net/sites/veritas_d/files/Data%20Protection%20Act%205%20of%202021.pdf

**The collection, storage, and use of biometric data and personal information raise significant privacy and data protection concerns.**

Organisations must have a lawful basis for processing biometric data and must obtain explicit consent from individuals before collecting or using this data unless an exception applies. They must also implement appropriate security measures to protect biometric data from unauthorised access or disclosure.

## Citizenship, the basis of ID systems in Zimbabwe

In Zimbabwe, identity systems are closely linked to the concept of citizenship. Zimbabwe's current Constitution adopted in 2013, sets out three categories of citizenship, namely, by birth, by descent and by registration. Citizens have a right to identity documents. The Constitution states:

"..... all Zimbabweans citizens are entitled to the following rights and benefits, in addition to any others granted to them by law:
(b) to passports and other travel documents and
(c) to birth certificates and other identity documents issued by the State." [4]

The issuance of the national ID documents is a statutory requirement in terms of the National Registration Act (Chapter 10:17)[5] which came into effect in 1976 but has been amended a total of six times - the last amendment being 22/2001. The Registrar General of National Registration established under this Act is responsible for the processing of identity documents and for verifying the authenticity of supporting documents submitted in an application.

Zimbabwe has a biometric identity system because each identity document contains a facial image and fingerprints captured during the registration process. The ID number itself is a unique 11/12-character alphanumeric number and one alphabet character assigned upon registration at birth and included in a birth certificate issued in terms of the Births and Deaths Registration Act (Chapter 5:02).

## Zimbabwe's biometric ID tapestry

Zimbabwe has implemented several biometric ID systems for various purposes, including voter registration, national identity cards, and border control.

The Biometric Voter Registration (BVR) system was implemented in 2017 to create a new voters' roll for the 2018 general elections. The system uses biometric data, including fingerprints and facial recognition, to register voters and eliminate duplicate registrations.

Zimbabwe's National Identity Card System uses biometric data, including fingerprints and facial recognition, to issue national identity cards to citizens. Similarly, the National Passport and National Drivers License are also forms of biometric identity which contain the same biometric data as the National Identity Card.

In December 2021, the government of Zimbabwe launched an updated biometric passport that contains a chip with the holder's personal information and biometric data, including fingerprints and facial recognition. Government has stated that this passport is more secure and tamper-proof than the previous passport, making it more difficult to forge or alter.

The Zimbabwe Border Control System uses biometric data, including fingerprints and facial recognition, to verify the identity of travellers entering and leaving the country. The system was implemented to enhance border security and prevent illegal immigration and human trafficking.

The government has also conducted a biometric registration of civil service workers in Zimbabwe in order to create a digital record of their identity. The purpose of the biometric registration is to enhance the accuracy and integrity of the civil service payroll system by eliminating ghost workers and reducing payroll fraud.

4 Chapter 3 of Zimbabwean Constitution.
5 https://www.law.co.zw/download/1744/

The biometric registration of civil service workers was initiated by the Zimbabwean government in 2015 as part of a broader public sector reform agenda. The government mandated all civil servants to undergo biometric registration, which involved capturing their fingerprints and facial images. The data was then stored in a centralized database for use in payroll processing.

The biometric registration process was carried out in phases, with different groups of civil servants being registered at different times. The registration exercise was conducted by the Civil Service Commission in collaboration with the Registrar-General's Office, which is responsible for issuing national identity documents.

There are several advantages of biometric identity systems. Broadly, biometric identity systems can offer improved security, convenience, efficiency, accuracy, and fraud prevention compared to traditional methods of identity verification.

While biometric identity systems offer several advantages, there are also some potential disadvantages to consider. Biometric data is highly sensitive and personal, and individuals may be concerned about the security and privacy of their biometric data. Biometric data can be used to track individuals and reveal sensitive information about their health, habits, and lifestyle. In addition, biometric databases on which biometric date is stored are vulnerable to hacking and other cyber threats, and once compromised, biometric data cannot be changed like a password or PIN.

Biometric identity systems are not infallible, and errors can occur. False positives can occur when the system incorrectly identifies someone as a different individual, while false negatives can occur when the system fails to identify an individual correctly.

Cost implications must also be considered as biometric identity systems can be expensive to implement, requiring specialised hardware and software and maintenance, as well as staff training.

Not all individuals may be able to use biometric identity systems, such as those with physical disabilities or medical conditions that affect their biometric data.

## Important considerations

It is important that any storage and use of biometric data for surveillance purposes is subject to appropriate legal and regulatory frameworks that ensure accountability, transparency, and respect for human rights. Any such use must be necessary, proportionate, and grounded in law, and individuals must be informed about the purposes and scope of the surveillance, as well as their rights and protections under the law. But Zimbabwe does not have adequate frameworks to safeguard biometric data and biometric databases.

In the absence of safeguarding frameworks, it is possible that the government of Zimbabwe may repurpose biometric databases for surveillance purposes, raising significant privacy and human rights concerns. Biometric data is highly sensitive and personal, and the use of such data for surveillance purposes without appropriate legal safeguards is a violation of individuals' privacy rights.

The repurposing of biometric databases for surveillance could also have a chilling effect on free speech and other human rights, as individuals may be less likely to express themselves or engage in peaceful protests if they believe they are being monitored and surveilled by the government.

## Digital IDs: the case of Zimbabwe

As indicated, biometric IDs rely on the unique physical characteristics of an individual, such as fingerprints, iris scans, facial recognition (photos), or voiceprints. Biometric IDs are typically more secure and difficult to forge or steal than traditional forms of identification, such as ID cards or passports. Biometric IDs can be used for a variety of purposes, such as border control, voter registration, or access control to secure areas.

On the other hand, a digital ID is a form of identification that relies on digital credentials, such as a username and password, digital certificates, or smart cards.

These credentials are issued by a trusted authority and can be used to authenticate the identity of an individual for a variety of purposes, such as online transactions, access to secure systems, or digital signatures.

The main difference between digital ID and biometric ID is that digital ID relies on digital credentials issued by a trusted authority, while biometric ID relies on the unique physical characteristics of an individual.

Zimbabwe has taken measures to digitise identity systems such as the national ID system by adding security features to the card (e.g., ultraviolet fluorescence, dynamically shifting ink, holograms, watermarks, fingerprints and security barcodes), but the country is yet to have a digital foundational ID system.

## Pros and cons of digital IDs

The impact of digital ID and biometrics on digital rights is a complex issue that has both positive and negative implications. On the one hand, digital ID and biometric systems have the potential to enhance security, reduce fraud, and improve access to essential services, such as healthcare and financial services. These systems can also facilitate the delivery of public services and enable governments to better monitor and evaluate policy outcomes.

However, digital ID and biometric systems can also have negative implications for digital rights.

The collection, storage, and use of biometric data and personal information raise significant privacy and data protection concerns. The misuse or unauthorised access to such data could have serious consequences for individuals' privacy rights.

Biometric systems may disproportionately impact marginalised groups and perpetuate existing biases and discrimination.

For example, facial recognition technology has been shown to have higher error rates for women and people of colour, leading to false identification and potential harm. Digital ID and biometric systems may exclude individuals who do not have access to technology or who are unable to provide the required biometric data, such as refugees or people with disabilities. This can exacerbate existing inequalities and limit access to essential services.

Biometric and digital ID systems possess the capability to provide detailed insights into an individual's activities, behaviors, and movements. Through these systems, governments can potentially track and analyse citizens' movements, interactions, and transactions. While this level of surveillance might be aimed at enhancing security or streamlining services, it also raises significant concerns regarding personal privacy and freedom of movement.

This level of monitoring has the potential to erode the expectation of privacy that individuals have in their daily lives. Continuous tracking through biometric and digital IDs could lead to the creation of comprehensive profiles detailing an individual's habits, routines, associations, and even preferences. Consequently, this heightened surveillance may impinge upon the fundamental right to privacy, potentially creating a chilling effect on personal freedoms.

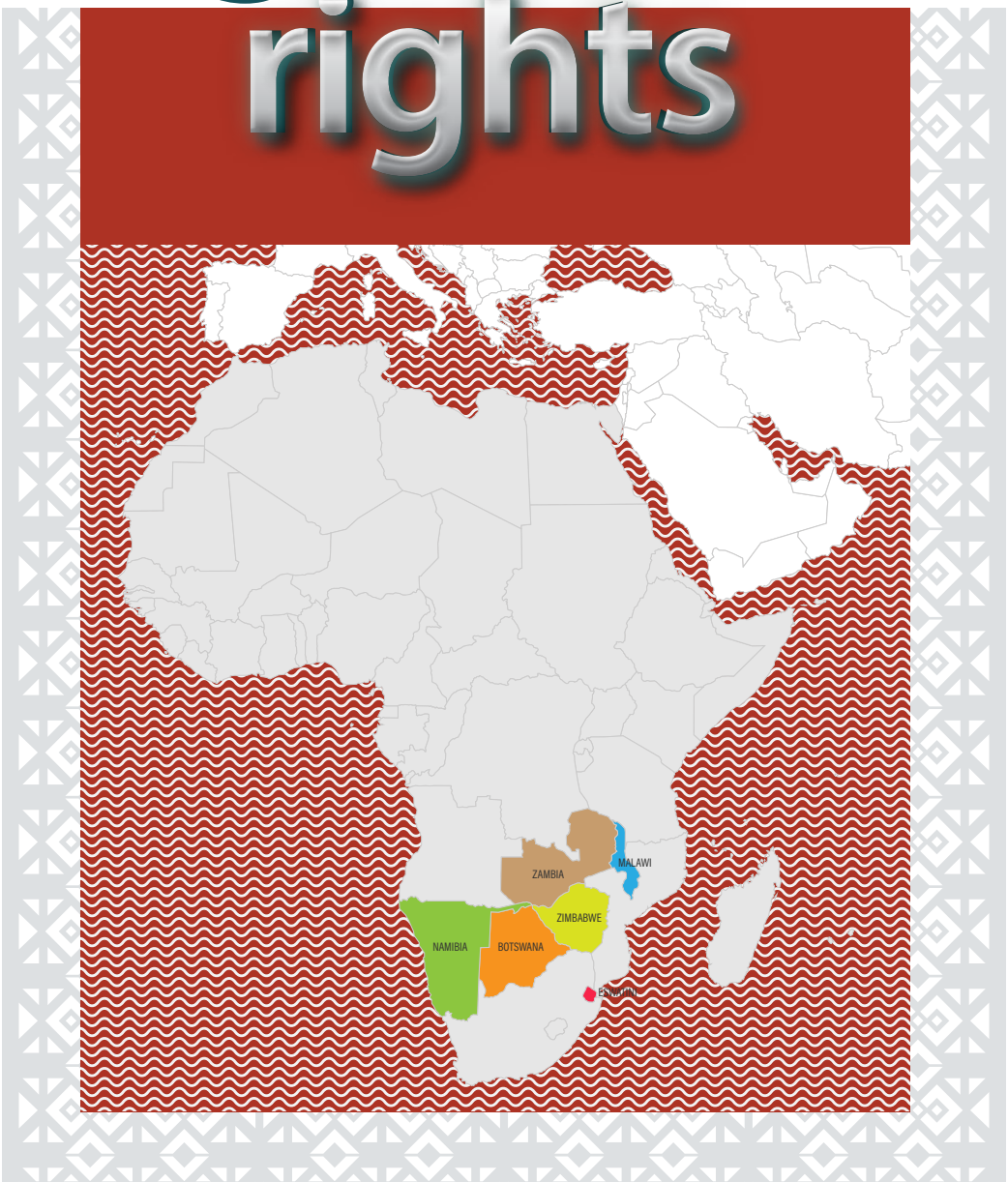
Moreover, the constant monitoring of citizens' behavior and movements could be seen as a form of intrusive oversight by the government. It might create an environment where individuals feel inhibited in their actions, limiting their freedom of movement and expression due to the awareness of being constantly monitored. ■

6 Digital Identity in Zimbabwe: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa https://researchictafrica.net/wp/wp-content/uploads/2021/11/Zimbabwe_31.10.21.pdf

### References


1. General Data Protection Regulation: https://gdpr-info.eu/
2. https://www.veritaszim.net/sites/veritas_d/files/Data%20Protection%20Act%205%20of%202021.pdf
3. Chapter 3 of Zimbabwean Constitution.
4. https://www.law.co.zw/download/1744/
5. Digital Identity in Zimbabwe: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa https://researchictafrica.net/wp/wp-content/uploads/2021/11/Zimbabwe_31.10.21.pdf

# digital rights SOUTHERN AFRICA




MISA BOTSWANA · CANGO · MISA MALAWI · nmit FREE SPEECH FOR AFRICA · MISA ZAMBIA · MISA ZIMBABWE

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS · OSISA Open Society Initiative for Southern Africa · AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS