

digital

SOUTHERN AFRICA

Issue No. 02

FEBRUARY 2024

rights



Privacy at Risk: Challenges to Data and Online Security

Eswatini strives for digital sovereignty amid technological advancements

▶ pg 10

Unregulated CCTV in Zambia sparks data privacy concerns

▶ pg 22

Zimbabwe's digital leap falls short in bridging access to justice gaps

▶ pg 26

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

▶ **04** **Editorial**
A region grappling with digital rights deficits
By Frederico Links

▶ **06** **Botswana showcases e-government's privacy pitfalls**
Privacy Threats in Botswana's E-Government Initiatives: Surveillance, Arrests, and Data Violations Despite Existing Laws.
By Thapelo Ndlovu

▶ **12** **Eswatini strives for digital sovereignty amid technological advancements**
Eswatini's 2022 Cyber Laws Raise Concerns Over Press Freedom and Social Media Criticism Amid Privacy Standards Push.
By Ndimphiwe Shabangu

▶ **15** **Unveiling the landscape: Malawi's data protection journey and the evolving digital rights terrain**
Data Protection Challenges in Malawi: Call for Independent Authority Amidst Delayed Legislation.
By Jimmy Kainja

▶ **20** **Rights watered down in draft privacy and data protection bill in Namibia**
Namibia's Latest Privacy Bill Draws Criticism for Weakened Data Subject Protections.
By Frederico Links

▶ **24** **Unregulated CCTV in Zambia sparks data privacy concerns**
Zambia Drafts Legislation to Regulate CCTV for Privacy and National Security.
By Mwazi Sakala & Maureen Mulenga

▶ **28** **Zimbabwe's digital leap falls short in bridging access to justice gaps**
Zimbabwe Judiciary's Digital Transformation Faces Challenges in Access and Security.
By Nompilo Simanje

digital rights

SOUTHERN AFRICA

ISSUE 02

FEBRUARY 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

Copy editors:

Reyhana Masters
Lis Jordan

Layout & production:

Naua Web Trading

Cover picture:

EV, Unsplash

Contributors:

Thapelo Ndlovu (Botswana)
Ndimphiwe Shabangu (Eswatini)
Moses Kaufa (Malawi)
Frederico Links (Namibia)
Mwazi Sakala (Zambia)
Maureen B. Mulenga (Zambia)
Nompilo Simanje (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

A region grappling with digital rights deficits

F R E D E R I C O L I N K S

Throughout 2023 signs and episodes of shrinking civic space continued to mark the Southern African digital rights landscape.

Perhaps the starkest example of this regionally was the dramatic raid on one of Botswana's leading newspapers, Mmegi, by state security agents and the arrest and brief detention of two journalists for unspecified reasons. During the arrest the mobile phones and computers of the journalists were confiscated and withheld even after the journalists had been released.

The situation was such a violation that the Committee to Protect Journalists (CPJ) Africa coordinator, Angela Quintal, stated in response: "It is particularly concerning that the journalists have not received their electronic devices back from authorities, given Botswana's abuse of digital forensic tools that compromise journalists' sources."

This episode of media and digital rights remains largely unresolved and has heightened concerns about a deteriorating human rights environment in a country once regarded a democratic beacon for the rest of the continent.

The article from Botswana in this edition, by Thapelo Ndlovu, exploring the country's struggles with implementing data and privacy protections, in the face of the increasing roll-out of e-governance systems, reflects on the dark clouds that have gathered over the Botswana digital rights landscape.

The same and similar clouds of concern are gathering over countries across the region – in Namibia a proposed data protection bill fails to adequately provisions for the rights of data subjects; in Eswatini, as in Botswana, free expression and media freedom online are constantly under threat as the state tries to assert its sovereignty; in Malawi the struggles reflect a region-wide grappling with trying to come up with and implement a data and privacy protection framework that speaks to local realities; in Zambia there's growing unease with the introduction of public surveillance systems that could be undermining of basic human rights in the absence of regulatory safeguards; and in Zimbabwe, which has become emblematic of the threat situation regionally, access to justice digitally is a frontier which has its challenges.

What this edition serves to spotlight is that privacy and data protections remain and will continue to remain areas that regional civil societies have to be seized with going forward. The same with access to internet and telecommunication services.

What this edition serves to spotlight is that privacy and data protections remain and will continue to remain areas that regional civil societies have to be seized with going forward. The same with access to internet and telecommunication services.

And what should also not be lost sight of, and which should shine through the articles in this edition, are that activists, journalists, and ordinary citizens face threats and challenges to their privacy, data security and access to digital services and spaces.

It should be clear, that while this edition speaks to contexts across six countries the issues discussed reflect trends and practices playing out across the whole Southern African Development Community (SADC) region to greater or lesser degrees.

Some of these trends and practices are continental as well and are topical in discussions of the state of human rights on the continent. Advocacy efforts around these topics and issues remain substantial and strategically significant.

We invite you to read and engage with the content of this edition of the digest, and to reflect on what is happening against the backdrop of what is unfolding where you are.

Good reading! ■





Botswana showcases e-government's privacy pitfalls



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

Privacy Threats in Botswana's E-Government Initiatives: Surveillance, Arrests, and Data Violations Despite Existing Laws

Botswana's venture into electronic government traces back to 2007 with the adoption of the Maitlamo Information and Communication Technology (ICT) Policy (Moahi, 2014).¹ Since then, both digitisation and digitalisation² have been integral parts of government policy and have recently been highlighted as the third priority in the current government reset agenda.³

Former Deputy Permanent Secretary in charge of information and media, Dr. Jeff Ramsay, highlighted, "E-government was made a top government program in 2008, aligning with global trends."⁴ However, he lamented its limited progress, citing challenges due to conflicting visions and interests.

Nevertheless, there's been consistent political discourse, as Nkwe (2012)⁵ notes, indicating Botswana's dedicated efforts toward promoting e-government. Sebina and Zulu (2014)⁶ view e-government as a means to prioritize citizens. They refer to Carbo's (2007) three phases for successful e-government: access to information, its effective utilization, and public trust in such information. These expectations could materialise with assured privacy and data protection, along with equitable access to digitisation, thereby ensuring full participation (digitalisation).

Bante et al (2021)⁷ in a discussion paper, titled 'E-government and democracy in Botswana: Observational and experimental evidence on the effects of e-government usage on political attitudes', provide what they call three mechanisms by which e-government may affect people's attitudes towards government or the system. These they mention as, first, an 'empowerment mechanism', in which issues of accessibility and citizen empowerment are realised; second, an 'appeasement mechanism', in which e-government may bloat citizens' satisfaction with the government; and, lastly, an 'equal treatment mechanism', in which the trust in systems is enhanced as citizens are likely to be treated fairly and equally (Bante et al 2021).

This article explores whether e-government in Botswana ensures privacy and protects personal data. E-government collects personal information, which if mishandled, might pose a threat to democracy.

Bante et al (2021) highlighted concerns that digital tools enabling increased surveillance might compromise democracy. Moreover, in Africa, including Botswana, there are hurdles to e-government. Nkwe (2012), citing Alshehri and Drew (2010), identifies challenges like inadequate ICT infrastructure, as well as security and privacy issues.

-
- 1 <https://www.igi-global.com/chapter/e-government-development-in-botswana>
 - 2 Digitisation is the specific act of converting analogue information to digital form, while digitalisation involves the broader transformation and utilization of digital technologies to innovate or improve processes, services, or systems.
 - 3 <https://yourbotswana.com/2021/05/30/the-new-reset-priorities-for-the-government-of-botswana/>
 - 4 <https://www.un.org/en/development/desa/publications/global-e-government-survey-2008.html>
 - 5 https://www.academia.edu/31833702/E_Government_Challenges_and_Opportunities_in_Botswana
 - 6 <https://www.igi-global.com/chapter/botswanas-e-government-programme/107174>
 - 7 https://www.idos-research.de/uploads/media/DP_16.2021.pdf

The case of Botswana

For a long time, Botswana has received favourable international ratings in terms of transparency, rule of law, freedoms and prudent economic management. However, Civicus Monitor (2021) observed a decline from a 'Narrowed' rating to 'Obstructed' in liberties, citing, among others, surveillance of citizens⁸. In recent years, the country experienced several detentions and arrests of individuals under cyber related laws. The Cyber Crime and Computer Related Crimes Act of 2018⁹ has been used to stifle digital expression, along with Section 44 of the Corruption and Economic Crime Act of 1994¹⁰.

While there is increased digitisation across all sectors, and widespread use of social media, there have also been disturbing incidents of surveillance, resulting in detention of journalists¹¹ and other users. The confiscation of the mobile phones of journalist Tsaone Basimanebotlhe in 2019¹² and Reverend Thuso Tiego in 2021¹³ were among such incidents. Basimanebotlhe was reportedly detained, and her devices confiscated because state security agents were looking for the sources behind an article in which photos of some agents had been published. Tiego was reportedly arrested, and his phones confiscated for allegedly violating the Public Order Act of 1967, with the police claiming they needed his phones for their investigations. Tiego's lawyers have since indicated that they intended suing the state on his behalf¹⁴.

Domestic, regional and international frameworks

The Botswana Constitution, in Section 12, protects freedom of expression, including access to information. The protection of the right to privacy is also guaranteed in Section 9, which reads:

"Except with his or her own consent, no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises."¹⁵

Aside from the constitution there are a number of laws and policies that impact on digital rights, and specifically the right to privacy, in Botswana. These frameworks can be clustered into enabling and disabling laws and policies. Enabling laws and policies are those that are relatively consistent with the constitution, while disabling laws and policies appear to be inconsistent with the constitution.

Enabling laws and policies

- Maitlamo ICT Policy – This policy was adopted in 2004 and was meant to facilitate ICT rollout in the country;
- Data Protection Act (DPA) of 2018 – this law was meant to provide protections in terms of privacy and personal data. It was only operationalised in October 2021¹⁶ and to date some parts have not been fully implemented, although the Information Commissioner has been appointed.

Disabling laws and policies

- Corruption and Economic Crime Act of 1994 – This law has been used to confiscate the electronic devices of journalists, such as those of Botswana Gazette journalists;¹⁷
- Public Service Act of 2008 – This law has various sections that bar public servants from disclosing government information.

8 <https://findings2021.monitor.civicus.org/country-ratings/botswana.html>

9 <https://www.bocra.org.bw/cybercrime-and-computer-related-crimes-act-2018>

10 <https://inkjournalism.org/51/botswana-in-the-grip-of-bad/>

11 <https://cpj.org/2022/05/botswana-journalists-remain-vigilant-under-new-surveillance-law/>

12 <https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/>

13 <https://www.mmegi.bw/news/rev-tiego-jailed-to-appear-in-court/news/>

14 <https://www.facebook.com/photo?fbid=563993185328783&set=pcb.563993258662109>

15 <https://www.parliament.gov.bw/images/constitution.pdf>

16 <https://otlaadisa.law/the-data-protection-act-comes-into-effect>

17 <https://amabhungane.org/stories/botswana-gazette-journalists-arrested-over-story/>



- Cyber Crime and Computer Related Crimes Act of 2018 – This law has been used to clamp down on freedom of expression online. It is widely cited in charge sheets¹⁸;
- Criminal Procedure and Evidence (Controlled Investigations) Act of 2022 – A new law that, as a bill, threatened unfettered surveillance and invasion of privacy. Threatening provisions were watered down following public outcry¹⁹ before the law was enacted.

Regional and International frameworks

Botswana is a signatory to the United Nations’ Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, as well as the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention)²⁰, although it has not ratified it yet.

Status of the Data Protection Act (DPA) of 2018

With regard to implementation of the data protection law, to date an Information Commissioner has been appointed and is in the process of setting up a fully-fledged secretariat. While the law ostensibly provides protections for online privacy and personal data, it contains significant exemptions that negate its purpose. Section 3 (b) of the law provides for the exemption of the processing of personal information “by or on behalf of the state where the processing involves national security, defence or public interest” from the provisions of the law.

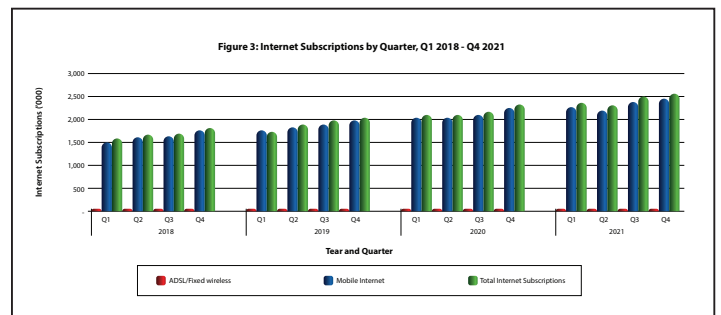
According to the Africa Cyber Security Report of 2020/21, 55% of people surveyed in Botswana were aware of the data protection law. The findings of the report were released by the government-owned Botswana Fibre Network (BOFINET) in June 2022²¹.

Internet access and affordability

Public perception is that internet connectivity in Botswana is expensive and slow²². However, the regulator, the Botswana Communications Regulatory Authority (BOCRA), has maintained that the perception was misinformed.

According to Statistics Botswana’s 2021 fourth quarter (Q4) ICT Statistics Brief, subscriptions of mobile and fixed-line internet increased by 3.4% and 4.6%, respectively, over the third quarter of that year. While fixed-line internet subscriptions remained relatively low, at 101,915 (Q4 2021), up from 97,395 (Q3 2021), mobile internet subscriptions climbed to 2.45 million, up from 2.37 million in Q3 2021²³.

The figure below shows internet subscriptions from Q1 2018 to Q4 2021.



Source: Statistics Botswana

E-government in Botswana

There are both positive and negative outcomes associated with the rollout of e-government. While it is proposed to provide better service to citizens and residents, it also provides the mechanisms for human rights violations, such as abusive intrusions into privacy.

18 <https://cpj.org/2021/05/news-editor-botswana-jail-facebook/>

19 <https://freexpression.org.za/a-threat-averted/>

20 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

21 <https://www.nbfira.org.bw/bofinet%E2%80%99s-stakeholder-engagement-data-protection-act-and-digital-data-centre>

22 <https://www.bocra.org.bw/sites/default/files/documents/Understand%20Broadband%20Connectivity.pdf>

23 <https://statsbots.org.bw/sites/default/files/publications/Q4%202021%20ICT%20Stats%20Brief.pdf>

The Botswana government's surveillance practices have become a threat to the acceptance and uptake of e-government services, as more and more people are charged on the basis of information obtained through surveillance

Opportunities

According to Bante et al (2021), the Botswana government has been introducing one strategy after the other in order to provide universal access to services. The 2015-2021 e-government strategy made provision for several e-government services to be established, such as "online payment systems for water and electricity services; the possibility of individual income or VAT returns; Botswana e-laws and digital livestock identification and trace-back system for cattle". Other notable proposed e-services were downloadable government forms from government websites.

Threats

The Botswana government's surveillance practices have become a threat to the acceptance and uptake of e-government services, as more and more people are charged on the basis of information obtained through surveillance²⁴.

Ramsay believes this is not unique to Botswana, stating that privacy is under threat globally even in jurisdictions such as most of the European Union (EU), with whistleblower and data protections. Global mass surveillance is the new normal.

In mid-2022, a letter from the Directorate of Intelligence and Security Services (DISS) circulated on social media, in which the DISS demanded CCTV footage from a Gaborone restaurant. The letter, dated 14 June 2022, request that DISS be furnished with hard drives containing CCTV footage, or any other storage equipment which accommodates and or captures live footage of your restaurant."

The fear expressed online at the time was that the demand for CCTV footage would expose all guests of the restaurant to potential privacy invasions by the security service.

In another case from 2022, the Botswana Mining Workers Union (BMWU) notified Debswana, which is jointly owned by the Botswana government and the De Beers Group of Companies, of its intention to sue over violations of the right to privacy of mineworkers (The Voice, 19 June 2022).

This followed a court ruling in favour of a company, Infotrac, which had sued Debswana over payment for surveillance services valued at P100 million (±US\$10 million). The union considered evidence presented in the Infotrac case as confirmation that workers had been illegally spied on and their right to privacy violated by Debswana²⁵. This ruling was overturned later.

On top of concerns around pervasive state surveillance, another challenge to acceptance and use of e-government services in Botswana is continuous power outages and the 'system is down' syndrome. Botswana government systems appear to be down regularly and therefore cannot provide e-government services uninterrupted. Sambona (2010) claims that these continuous system failures are due to poor maintenance and infrastructure²⁶.

Human rights approach

A human rights approach would entail the PANEL principles of Participation, Accountability, Non-discriminatory, Equality, Empowerment and Legality.

24 <https://www.haaretz.com/israel-news/tech-news/2021-07-14/ty-article/premium/cellebrite-tech-used-against-journalists-in-botswana-investigation-reveals/0000017f-db5a-d3a5-af7f-fbfe72930000>

25 <https://news.thevoicebw.com/miners-threaten-to-sue-debswana/>

26 https://globaljournals.org/GJHSS_Volume19/1-E-Government-A-Tool-for-Service-Delivery.pdf

Some of the rights that the DPA provides for the data subjects are the right to withdraw consent, the right to access their information through processor or controller, as well as the right to be informed about the processing of their data.²⁷

What is more pronounced in the DPA from the perspective of human rights is a dominating political control.

Botswana's DPA has significant involvement of the minister. Section 6 (1) gives the minister power to appoint the commissioner and the deputy commissioner while the rest are appointed by the commissioner. This goes against the principles of citizen participation in the establishment of the commission as espoused by various treaties. The minister further has a leeway in giving directions to the commissioner as stated in Section 9. The minister also appears in the appointment of all members of the Appeals Tribunal in Section 45. Section 53 continues to give the minister a blank cheque as s/he can make regulations, "prescribing anything under this Act which is to be prescribed or which is necessary for the better carrying out of the objects and purposes of this act or to give force and effect to its provisions."

The law, however, provides an element of accountability in the sense that a data controller or processor could be taken to task and face hefty fines for contravening the act according to subsections under Section 51.²⁸

Former army top official, Pius Mokgware brought a matter before court accusing his former employers of conducting surveillance on him. He further sued Be Mobile telecommunications company to produce evidence that there was, "systematic monitoring and tapping of phone calls, communications from his cellular phone and general surveillance."²⁹

Conclusion

Instances of violation of privacy rights and personal data protection exist in Botswana. The advent of e-government without proper guidelines and awareness of privacy rights has exposed personal data to abuse.

The delay in implementing the 2018 DPA has added to the uncertainty in the industry and raised concern over government's intentions. This is made worse by formulation of other laws which are inconsistent with the ideals of the rights to privacy and personal data protection. The unfettered exemptions in the DPA dilute the spirit of the act and their amendments as promised by the Information Commissioner are eagerly awaited. For E-government to succeed, it must be human rights oriented and mechanisms be put in place to ensure that it is. E-government involves mass collection of personal data and without the implementation of the DPA, the benefits of digitalisation may not be optimised.

From the research conducted by Africa Cyber Security (2020-21)³⁰, indications are that personal data is not handled with care and organisations do not invest in enlightening their personnel on security issues.

It is also evident from the DPA that there is space for political interference in the running of the commission. With key commissioners and the whole Appeal Tribunal appointed by the minister, power is congested in one person, and this is inconsistent with principles in the African Declaration of Internet Rights and Freedoms and others. With the government being the largest user of personal information, having a minister as a gatekeeper of possible abuse is too much of conflict of interest and defeats the spirit of the data protection principles.

Food for thought

In light of the conclusion, the following is recommended, that:

- The implementation of the DPA be sped up;
- E-government be rolled out with protective mechanisms such as a code of conduct for employees;

27 <https://caseguard.com/articles/ensuring-data-protection-and-privacy-in-botswana>

28 <https://otlaadisa.law/the-data-protection-act-comes-into-effect>

29 <https://www.sundaystandard.info/details-of-bdf-intelligence-illegal-spying-on-former-deputy-commander-kept-secret/>

30 <https://cybersecuritymag.africa/autorite-protection-donnees-afrique-etat-des-lieux-par-pays>



- The DPA be amended to counterbalance the exemptions extended to the state;
- E-government instruments be consistent with human rights and right to privacy and personal data protection;
- Public education in the form of mass communication advertorials be undertaken to sensitize the public about privacy rights and data protection;
- A specific pamphlet of guidelines on issues to consider when dealing with personal data be produced for public officials;
- Organisations, including government, be encouraged to train staff who handle personal data on security and human rights implications;
- Civil society organisations be involved in public education and be on alert for violations. ■

** For the purposes of this article, e-government shall mean any electronic service both within and outside government. It shall therefore be used interchangeably with e-service in the government.*

References

<https://www.igi-global.com/chapter/e-government-development-in-botswana>

<https://yourbotswana.com/2021/05/30/the-new-reset-priorities-for-the-government-of-botswana/>

Global E-Government Survey 2008 | Latest Major Publications - United Nations Department of Economic and Social Affairs

<https://www.semanticscholar.org/paper/E-Government%3A-Challenges-and-Opportunities-in-Nkwe/e86332923fc092fdca4067ec941b1434f4774e76>

<https://www.igi-global.com/chapter/botswanas-e-government-programme/107174>

<https://www.idos-research.de/discussion-paper/article/e-government-and-democracy-in-botswana-observational-and-experimental-evidence-on-the-effect-of-e-government-usage-on-political-attitudes/>

<https://findings2021.monitor.civicus.org/country-ratings/botswana.html>

<https://www.bocra.org/bw/cybercrime-and-computer-related-crimes-act-2018>

<https://inkjournalism.org/51/botswana-in-the-grip-of-bad/>

<https://cpj.org/2022/05/botswana-journalists-remain-vigilant-under-new-surveillance-law/>

<https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/>

<https://www.mmegi.bw/news/rev-tiego-jailed-to-appear-in-court/news/>

<https://www.facebook.com/photo?fbid=563993185328783&set=pcb.563993258662109>

<https://www.parliament.gov.bw/images/constitution.pdf>

<https://otlaadisa.law/the-data-protection-act-comes-into-effect>

<https://cpj.org/2021/05/news-editor-botswana-jail-facebook>

<https://freeexpression.org.za/a-threat-averted/>

<https://amabhungane.org/stories/botswana-gazette-journalists-arrested-over-story/>

https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

<https://www.nbfira.org/bw/bofinet%E2%80%99s-stakeholder-engagement-data-protection-act-and-digital-data-centre>

<https://www.bocra.org/bw/sites/default/files/documents/Understand%20Broadband%20Connectivity.pdf>

<https://statsbots.org/bw/sites/default/files/publications/Q4%202021%20ICT%20Stats%20Brief.pdf>

<https://www.haaretz.com/israel-news/tech-news/2021-07-14/ty-article/.premium/cellebrite-tech-used-against-journalists-in-botswana-investigation-reveals/0000017f-db5a-d3a5-af7f-fbfe72930000>

<https://www.facebook.com/search/top?q=cctv%20at%20rhaphsody>

<https://news.thevoicebw.com/miners-threaten-to-sue-debswana/>

https://globaljournals.org/GJHSS_Volume19/1-E-Government-A-Tool-for-Service-Delivery.pdf

<https://caseguard.com/articles/ensuring-data-protection-and-privacy-in-botswana>

<https://otlaadisa.law/the-data-protection-act-comes-into-effect>

<https://www.sundaystandard.info/details-of-bdf-intelligence-illegal-spying-on-former-deputy-commander-kept-secret/>



Photo credit: The Humanitarian

Eswatini strives for digital sovereignty amid technological advancements



NDIMPHEWE SHABANGU

Eswatini's 2022 Cyber Laws Raise Concerns Over Press Freedom and Social Media Criticism Amid Privacy Standards Push

Between June and July 2021, Eswatini experienced political upheaval, largely stemming from multiple governance issues worsened by the impact of COVID-19. The rise of digital media notably exposed societal awareness to the governance flaws within the political system and its leaders.


In Eswatini, two pivotal legislative measures impact internet governance: the Computer Crime and Cyber Crime Act of 2022 and the Data Protection Act of 2022.

Enacted in 2022, these laws underwent a consultative phase wherein civil society organizations actively contributed submissions. Notably, these inputs led to revisions in the legislation, which was still in its draft form (Bill) at the time. Concerns loom over potential implications of these statutes, particularly the perceived threat to press freedom and the possible curtailment of social media criticism directed at the government.

The Eswatini Communications Commission serves as the regulatory authority overseeing the communication sector within the country. Its purview encompasses telecommunications, broadcasting, postal services, and the management of radio spectrum frequencies. This mandate is delineated by the Swaziland Communications Commission Act No. 10 of 2013.¹

The period of unrest witnessed in June–July 2022 prompted the government to issue directives to various service providers—namely, the state-owned Eswatini Post and Telecommunications Corporation, along with private entities MTN Eswatini and Eswatini Mobile—to suspend internet services.

¹ <https://www.esccom.org.sz/about/profile/>



The proposed structure of the Data Protection Office weakens its financial, decision-making, and institutional independence. Malawi should consider establishing an independent Data Protection Commission or Authority outside MACRA.

In response to this action, the International Commission of Jurists drafted a letter directed at the CEO of MTN South Africa, urging the resumption of internet services within the affected region.²

Prior to that, in October 2021, during a period of protests in Eswatini, the government took measures to restrict access to various social media platforms. This action notably infringed upon the populace's fundamental right to access the internet. Such constraints not only impede the free flow of information but also pose a severe threat to civil society's ability to function openly and engage in free discourse. This imposition undermines the cornerstone of free speech and threatens to constrict the space for open dialogue and the free exchange of ideas, essential elements for an informed and participative society.³

Eswatini legislation and policies to ensure privacy and data protection

The Data Protection Act 2022 was passed at a critical time when the use of the internet and digitalisation rate increased in Eswatini. The Data Protection Act is a comprehensive piece of legislation which provides for the collection, processing, and disclosure of personal data.⁴ The Act is indicative that the government recognises the importance of data protection and privacy. Furthermore, to ensure this, the Eswatini Communications Commission is charged with regulating adherence to the Act and also has powers to sanction data controllers who breach this law. Section (6) (3) b indicates that the commission can impose administrative fines of up to five million Emalangeni (about USD268,000) for non-compliance by public or private party. Ibid. According to the Act, a data controller is a public or private body or any other person designated by law which determines the purpose and method for processing personal information. Ibid.

The Data Protection Act of 2022 holds significant importance as a legislative framework governing the handling of personal information, particularly in electronic formats, and the cross-border movement of such data beyond Eswatini's borders. A crucial aspect lies in Section 9(2), emphasizing the necessity of explicit consent from individuals for processing their personal data. However, certain sections, notably Section 36, raise concerns regarding potential interpretations that might encroach upon fundamental human rights, particularly in the context of reasons provided for non-action on filed complaints.

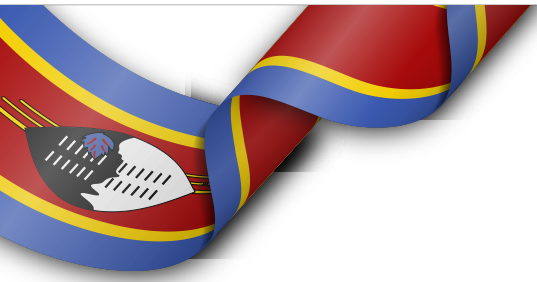
A comprehensive analysis of the Act indicates a balance between its positive and negative aspects. While certain provisions might raise apprehensions about potential rights infringement, the overall implementation of the Act is anticipated to significantly bolster privacy standards and data protection within the nation. The Act, by and large, stands poised to fortify the safeguarding of individuals' privacy and data rights in the country.

Section 44 of the Data Protection Act 2022 constitutes a pivotal aspect addressing unsolicited electronic communications. It grants citizens the right to halt direct marketing activities upon their request, extending to various forms of marketing, inclusive of digital platforms. Notably, individuals reserve the entitlement to lodge complaints regarding such marketing practices, directing these grievances to the Eswatini Communications Commission, which assumes responsibility for addressing and redressing these complaints.

2 <https://www.icj.org/wp-content/uploads/2021/07/ICJ-Letter-to-MTN-8.07.21.pdf>

3 <https://misa.org/blog/restoration-of-internet-and-social-media-services-in-eswatini/>

4 <https://www.esccom.org.sz/legislation/DATA%20PROTECTION%20ACT.pdf>



Moreover, a significant provision within this Act pertains to the prohibition of data collection from children. This crucial stipulation serves to safeguard minors by explicitly disallowing the gathering of their personal data without requisite permissions or legal authorisation.

Another imperative measure, amongst many, is section 17 (1) of the Data Protection Act 2022, which addresses notification of security breaches or compromises and states “Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the data controller, or any other third party processing personal information under the authority of a data controller shall notify (a) the commission; and the data subject unless the identity of such data subject cannot be established”. Ibid. In essence, this means that when a data breach has occurred where one’s data is stored (by a third party, data controller or an entity engaged to store data), one must be notified of such a breach.

The Computer Crime and Cyber Crime Act 2022 compliments the Data Protection Act 2022 in that it criminalises actions intended to manipulate, modify, or destroy data. An illustration is Section 6 of the Computer Crime and Cyber Act which addresses illegal data interference in which it is stated that on conviction, a fine not exceeding five hundred thousand Emalangeni or imprisonment of a period not exceeding three years or both may be applied.⁵ The Act also addresses data espionage, illegal system interference, computer related forgery and uttering, cyber terrorism, and many more issues which directly affect data protection and privacy.

The Data Protection Act 2022 encompasses Sections 32 and 33, specifically focusing on the regulation of trans-border movement of personal information outside the territorial bounds of Eswatini. These sections delineate protocols governing the transfer of personal data not only within the Southern African Development Community member states but also with non-member states.

This becomes crucial considering the ubiquitous nature of the internet, facilitating the unintentional transfer of Eswatini citizens' personal data to foreign jurisdictions.

Similarly, the Computer Crime and Cyber Crime Act 2022 in Section 31 introduces the concept of extra-territorial jurisdiction. In essence, this provision enables the prosecution of individuals for offenses committed under the Act, irrespective of their physical presence within Eswatini's borders. The rationale behind this measure stems from the reality that hackers, operating from abroad, can infiltrate networks, perpetrate cybercrimes, and abscond to other jurisdictions. The evolution of technological landscapes, including the advent of cloud computing and the proliferation of 5G networks, further amplifies the vulnerability to such cyber threats and data breaches.

Hence, advocating for public awareness campaigns centered on digital hygiene and safety assumes paramount importance in mitigating these risks and ensuring the protection of personal information in the digital sphere. ■

References

- www.freedomhouse.org/country/eswatini/freedom-world/2020
<https://www.chrpa.org/index.php/publications/>
<https://rsf.org/en/country/eswatini>
<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099248404262210321/idu05826bd7504b05041e60b07c0579f2b3ef617>
<https://www.esccom.org.sz/about/profile/>
<https://www.icj.org/wp-content/uploads/2021/07/ICJ-Letter-to-MTN-8.07.21.pdf>
<https://misa.org/blog/restoration-of-internet-and-social-media-services-in-eswatini/>
<https://www.esccom.org.sz/legislation/DATA%20PROTECTION%20ACT.pdf>
<https://www.esccom.org.sz/legislation/COMPUTER%20CRIME%20&%20CYBERCRIME%20ACT.pdf>

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



Unveiling the landscape: Malawi's data protection journey and the evolving digital rights terrain



M O S E S K A U F A

Data Protection Challenges in Malawi: Call for Independent Authority Amidst Delayed Legislation

Malawi was under British protection from 1891 to 1964, known then as Nyasaland, until it gained complete independence from the United Kingdom. It transitioned into a republic with a one-party governmental system in 1966, following a series of constitutional amendments. In 1994, a new constitution was enacted, introducing a bill of rights that paved the way for significant changes in the socio-political landscape, including the communications sphere¹.

This shifted to the creation of various policy instruments aimed at regulating communication services. Notable among these instruments are the Communications Act (initially drafted in 1998 and revised in 2016)², guiding the regulation of broadcasters and telecommunication firms, alongside the Electronic Transactions and Cyber Security Act of 2016³ and the Access to Information Act of 2017⁴. The implementation of the Communications Act established the Malawi Communications Regulatory Authority (MACRA), responsible for enforcing the Electronic Transactions and Cyber Security Act.

Since the early 1990s, Malawi has witnessed a surge in media organizations, outlets, and telecommunication companies. This period has seen significant growth in cellular phone usage and a remarkable expansion in Internet accessibility and usage.

The state of Internet Rights, Policy, and Governance

Malawi lacks a robust, currently enacted data protection law. However, data protection provisions are embedded in the Constitution of Malawi and outlined within the Electronic Transactions and Cyber Security Act of 2016 (referred to as 'the Act'). Section 21 of the Malawian Constitution grants every individual the right to personal privacy. This encompasses the right to be free from (a) personal, home, or property searches; (b) private possessions seizure; or (c) interference with private communications, including mail and all telecommunication forms.

Nevertheless, authorities are increasingly demanding citizens to surrender personal information for routine activities, ranging from using a mobile phone to participating in elections. The absence of a clear data protection law jeopardizes citizens' right to privacy.

-
- 1 [akn-mw-act-1994-20-eng-2020-11-03.pdf \(malawilii.org\)](#)
 - 2 [ACT41.PDF \(itu.int\)](#)
 - 3 [Electronic Transaction and Cyber Security Act 2016 - MACRA](#)
 - 4 [akn-mw-act-2017-13-eng-2017-02-16.pdf \(malawilii.org\)](#)



After the enactment of the January 2010 National Registration Act, the Malawian government initiated nationwide registration in 2017⁵. This mandates every Malawian aged 16 and above to enroll in the national register and acquire a national identity card.

According to the National Registration Bureau (NRB), the national ID system would serve many purposes by acquiring “information about the population” that would enable “policymakers to use data-driven planning” for development and services delivery. For individuals, this would give them “proof of their nationality and personal information so that they can use it to claim their benefits.”⁶

In January 2018, MACRA announced a mandatory national sim card registration exercise. Based on the Communications Act of 2016, this required everyone with a mobile phone number in the country to register their sim card. In July 2022, the Authority held a series of meetings with the media and other stakeholders announcing that they will soon embark on registration of mobile phone handsets.

MACRA says these registrations are important for several reasons: First, to prevent fraudulent practices; to recover stolen phones; offer protection from violence, threats, or hate texts; and check fraud and theft committed via mobile phones. Similarly, banks and telecommunication companies operating mobile money services embarked on a “know your customer” exercise in which Malawians were required to present their national ID for all transactions.

Data collected for the National Register includes a person’s surname and given names, nationality, date of birth, and place of birth. The NRB also collects data on one’s sex, current residence, height, eye colour, passport number, marital status and parents’ information. The bureau also collects biometric information, including all 10 fingerprints, a personal photograph and signature.

Meanwhile, there are a growing number of cases where people claiming to be from various organisations and financial institutions demand money from people⁷. It isn’t clear how these people obtained the personal information necessary, however, the suspicion is that information given registering agencies is not protected. This is just one of the dangers posed to individuals by the unregulated or uncontrolled collection, storage and use of personal data.

A Move towards Data Protection

The government of Malawi finalised the drafting of Data Protection Bill in June 2021.⁸ The aim of this Bill is to provide a comprehensive legislative framework for the protection and security of personal data, consolidate data protection provisions currently found in various Acts of Parliament, and protect the digital privacy of individuals without hampering social and economic development in the country. The Minister of Justice is yet to submit the Bill for cabinet approval.

In the words of CIPESA Analysis Report of the bill of May 2021, “Enacting the data protection law would represent fulfilment of the state’s obligation to protect the right to privacy of the individual and represent a key step towards meeting Malawi’s commitments under international human rights law”.⁹

Barriers to data protection, access and affordability of the internet

According to Kainja, 2019,¹⁰ “The improved access to and use of ICT, coupled with the aforementioned reforms have also allowed the government to adopt measures that curtail internet freedoms, including the criminalisation of online communication and massive collection of personal data.” These measures are enabled in part by retrogressive provisions in the 2016 Communications Act and the 2016 Electronic Transactions and Cyber Security Act.

5 National Registration (nrb.gov.mw)

6 <https://citizenshiprightsafrika.org/why-malawi-urgently-needs-a-data-protection-law/>

7 There are a growing number of cases where people claiming to be from various organisations and financial institutions demand money from people

8 Malawi-Data-Protection-Bill-final-draft-210630-.pdf (pppc.mw)

9 <https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Malawi-2019.pdf>

10 [google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiptMft6tqCAxXtY0EAHTiDDzsQFnoECBAQAQ&url=https%3A%2F%2Fwww.ajol.info%2Findex.php%2Fjh%2Farticle%2Fview%2F251334%2F237536&usg=AOwVaw1ASAVYNpK-T8j2B9d367Qm&opi=89978449](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiptMft6tqCAxXtY0EAHTiDDzsQFnoECBAQAQ&url=https%3A%2F%2Fwww.ajol.info%2Findex.php%2Fjh%2Farticle%2Fview%2F251334%2F237536&usg=AOwVaw1ASAVYNpK-T8j2B9d367Qm&opi=89978449)



The proposed structure of the Data Protection Office weakens its financial, decision-making, and institutional independence. Malawi should consider establishing an independent Data Protection Commission or Authority outside MACRA.

Internet freedom in Malawi has been affected by the limited state investment in ICT and internet infrastructure needed to facilitate affordable access to the internet, and the cost of internet services continues to rise. Since the current government led by President Lazarus Chakwera took office in 2020, there have been outcries that the cost of internet data must fall. Internet users in Malawi enjoyed unlimited data bundles with 40 Gigabytes at the highest speed of 5 megabytes per second costing about 35 United States Dollars for one month. However, in early August 2022 one mobile network provider announced increasing the price of the unlimited data bundles by almost 100 per cent.

Moreover, levies imposed on internet service providers and telecommunication companies exacerbate the challenges in achieving affordable internet access. The primary responsibility to enhance affordability lies with the government, as it holds the authority to legislate and ensure law enforcement. However, the government has yet to repeal or amend outdated laws from colonial and dictatorship eras that contradict human rights and impede media freedoms. These laws remain in effect, conflicting with the country's constitution.

While civil society demonstrates vibrancy in various social development realms, its proactive stance toward internet freedom and digital rights remains nascent. These issues are still emerging for many civil society organizations and human rights defenders in the country.

The regulator

The Malawi Communications Regulatory Authority (MACRA) regulates the country's telecommunication sector. It is mandated to make regulations and policies that govern the telecommunications sector.

The regulator issues operating licenses; monitors and enforces compliance with regulations; hears and determines disputes and complaints brought by industry or members of the general public; plans, controls and manages the frequency spectrum efficiently in order to maximise frequency availability; and protects the interests of consumers, purchasers and other users of communication services from unfair business practices, poor quality services and harmful or inferior products.

According to the draft Data Protection Bill, MACRA has the mandate for its enforcement.

Constitutional underpinning

The government initiated drafting of the Data Protection Bill, having realised that the country's economy is increasingly reliant on digital technologies and therefore there is a need to protect personal data of individuals collected, generated, stored and utilized 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.

The overall objective of this Bill is to regulate matters relating to personal data but does not apply to the collection or processing of personal data for personal, recreational or household purposes, or for security, law enforcement or public health purposes.

The data protection bill is aligned with international treaties Malawi is a party to, such as the International Covenant on Civil and Political Rights (ICCPR)¹¹, as well as the country's constitution, which is the supreme law of the country. The constitution has safeguards in its Bill of Rights that protect people's democratic rights.

11 International Covenant on Civil and Political Rights | OHCHR



Government, through the Bill, designates the Malawi Communications Regulatory Authority as the Authority to regulate and monitor personal data protection and digital privacy in Malawi and oversee the implementation of and be responsible for the enforcement of the Bill.

The Bill establishes a Data Protection Office within the Authority responsible for the activities relating to data protection under the Bill. From the onset, this arrangement may threaten the independence of the office. Setting up an independent Data Protection Commission because, while the Authority will be enforcing the law using the Communications Act and the Electronic Transaction and Cyber Security Act, the Data Protection Office will be focusing on protecting the public and adjudicating on complaints from the public about the same.

Similarly, the principles governing the processing of personal data should be applied in other sectors as well and in both public and private entities. The Bill requires a data controller or data processor to process data fairly and in a transparent manner and only where (a) the data subject has given and not withdrawn his consent, and (b) the data are required for legitimate purposes outlined in the Bill. The Bill further limits the processing of sensitive personal data.

Where the Bill empowers a data subject who is aggrieved by the decision, action or inaction of a data controller or data processor in violation of this Bill and or regulations, rules or other subsidiary legislation or orders to lodge a complaint with the Authority, there is need for an independent commission to initiate an investigation and not the Authority as outlined in the Bill.

The Bill proposes that Parliament should make this Bill the umbrella law on the protection and security of personal data in Malawi, by amending or repealing provisions related to personal data protection in two existing Acts of Parliament, namely, Access to Information Act, 2017 and Electronic Transactions and Cyber Security Act, to eliminate inconsistencies between this Bill and the said two Acts of Parliament.

Existing legal framework on Data Protection

The Electronic Transactions and Cyber Security Act. 2017

This Act defines personal data as “any information relating to an individual who_ (a) may be directly identified; or (b) if not directly identified, may be identifiable by reference to an identification number or one or several elements related to his physical, physiological, genetic, psychological, cultural, social, or economic identity.”

This law defines a data subject as “a person from whom data relating to that person is collected, processed or stored by a data controller.” Additionally, Section 74 requires data controllers to ensure that clients’ data is secure and is protected against accidents or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access by third parties, especially if the processing involves the transmission of data over a network.

The Communications Act of 2016

Under Section 176(1), the Act criminalises unlawful interception or interference by service providers, noting that, “a licensee operating an electronic communications network or providing an electronic communications service who, other than in the course of its duty, intercepts, interferes with the contents of, or modifies, any message sent as part of the electronic communications service, commits an offence and shall, upon conviction, be liable to a fine and imprisonment.”

The Access to Information Act of 2016

This Act provides for the right of access to information in the custody of public bodies and relevant private bodies as well as the processes and procedures for obtaining such information. Section 20(1) requires an information holder to notify third parties, if he considers that the information being requested relates to confidential or commercial interests, in writing with details of the request.



Third parties are required to respond in writing within 10 working days from the date of receipt of the notice and indicate whether they consider the information to be confidential and give reasons why the information should not be disclosed.

The National Statistics Act of 2013

Section 10 of the National Statistics Act, 2013 empowers the National Statistics Organisation (NSO) to collect all types of information, including personal information, nationwide on behalf of the government. While, Section 12(11) of the same Act states that the Commissioner or any authorised officer may, for any purpose connected to collecting statistical information, enter and inspect any land, building or other premises, vehicle, vessel or aircraft, it also says that they can only enter such areas with the consent of property owners or the backing of a warrant; and they are enjoined to maintain decency and order, including the protection of a person's right to dignity, freedom and privacy, under section 12(5).

Conclusion

The current legal and policy framework faces a significant challenge due to delays in enacting the privacy and data protection law. This delay becomes especially problematic amid heightened personal data collection and an increase in financial fraud cases within the country. Additionally, the privacy and data protection bill doesn't encompass national and multinational companies, including banks and telecommunication firms, which also handle data.

Regrettably, the existing draft laws on data protection lack adequate safeguards for resolving user complaints. The sole handling of all matters by the government Authority raises concerns about potential conflicts of interest in addressing complaints.

The proposed structure of the Data Protection Office weakens its financial, decision-making, and institutional independence. Malawi should consider establishing an independent Data Protection Commission or Authority outside MACRA.

Moreover, the Minister responsible for personal data protection and security should ensure that the bill mandates the inclusion of representatives from various sectors, such as human rights advocates, media organisations, doctors, lawyers, and other stakeholders in the regulatory framework. This inclusive approach would support the formation of an independent Data Protection Commission. The bill should also clarify the criteria for appointing a Data Controller.

The overdue Malawi Data Protection Act, despite commendable ongoing efforts, requires swift enactment by the parliament. Implementing the above proposals would ensure adequate protection of individuals' rights. ■

References

- Constitution of Malawi*, <https://www.wipo.int/edocs/lexdocs/laws/en/mw/mw030en.pdf>
- African Union, African Union Convention on Cyber Security and Personal Data Protection, Status List*,
- Electronic Transactions and Cybersecurity Act of 2016, Communications Act of 2016*
- <https://cipesa.org/2019/08/are-malawians-sleep-walking-into-a-surveillance-state/>
- State of Internet Freedom in Malawi 2019, Mapping Trends in Government Internet Controls, 1999-2019. January 2020* <https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Malawi-2019.pdf>
- 1. IMF Staff Country Reports Volume 184: Malawi: Economic Development Document (2017)
- 2. [akn-mw-act-1994-20-eng-2020-11-03.pdf](#) (malawilii.org)
- 3. ACT41.PDF (itu.int)
- 4. Electronic Transaction and Cyber Security Act 2016 - MACRA
- 5. [akn-mw-act-2017-13-eng-2017-02-16.pdf](#) (malawilii.org)
- 6. National Registration (nrb.gov.mw)
- 7. Malawi-Data-Protection-Bill-final-draft-210630-.pdf (pppc.mw)
- 8. <https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Malawi-2019.pdf>
- 9. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour-ce=web&cd=&ved=2ahUKewiptMft6tqCAxXtY0EAHTiDDzsQFnoECBAQAQ&url=https%3A%2F%2Fwww.ajol.info%2Findex.php%2Fjh%2Farticle%2Fview%2F251334%2F237536&usg=AOvVaw1ASAVYNpK-T8J2B9d367Qm&opi=89978449>
- 10. International Covenant on Civil and Political Rights | OHCHR



Rights watered down in draft privacy and data protection bill in Namibia

Sweeping changes to an earlier version means the latest draft is significantly weak on protecting data subjects



F R E D E R I C O L I N K S

Namibia's Latest Privacy Bill Draws Criticism for Weakened Data Subject Protections

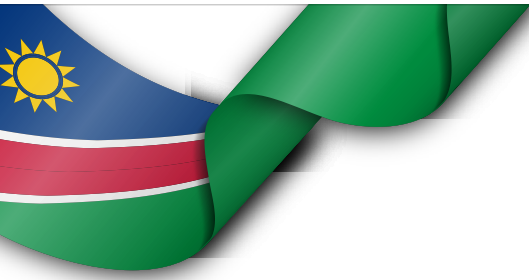
At the time of writing, Namibia still did not have an online privacy and data protection law on the statute books. However, such a law has been in on-and-off discussion within relevant Namibian government circles for most of the last decade, with an initial data protection bill even having been drafted in 2013.

It was only in 2018, though, that efforts towards crafting a substantive law had new life breathed into them when, under a year-long project running from October 2018 to December 2019, a cybersecurity capacity maturity assessment of Namibia was conducted as part of the Commonwealth Cyber Programme, by the World Bank and the Global Cybersecurity Capacity Centre, at the University of Oxford.¹

It was during this assessment that the prevailing online privacy and data protection situation in Namibia became clear, with the assessment report stating: "Most of the government agencies and private sector companies are not implementing any data protection standards and best practices to ensure that the sensitive and personal data that they collect, process and store are adequately protected."

Following this process, in 2020 a new consultation process was initiated, with assistance and technical support from the Council of Europe and the Commonwealth Secretariat, to help Namibia come up with an updated data protection draft bill². This process started off with a three-day workshop on data protection legislative drafting in February 2020 and culminated later that year with a draft bill that was shared as the "Final final Data Protection Bill 2020".

1 <https://cybilportal.org/projects/cmm-review-namibia-as-part-of-the-commonwealth-cyber-programme/>
2 https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/573WWxscOuZ5/content/glacy-cyber-security-and-cybercrime-maturity-assessment-of-namibia



Some of the areas of specific human rights concern raised about the 2022 draft were underdeveloped consent provisions, the almost complete absence of protections for data subjects, and the absence of carve-outs for journalistic, artistic and academic data collection and processing.

However, by the end of that year, the consultation and drafting process appeared to have stalled again and it was only in early October 2022 that momentum suddenly appeared to pick up again, when the Ministry of Information, Communication and Technology (MICT) suddenly, and quite unexpectedly for those interested in the topic, issued a notice calling for public inputs to a draft data protection bill to be submitted by 31 October.³

The bill for which inputs were being sought was quite substantially different from the last version that had been shared publicly – the “Final final Data Protection Bill 2020” version.

It is the version of the bill that became public in October 2022 that will be the focus of discussion in this article.

Domestic, regional and international frameworks

The right to privacy is enshrined in Article 13 of the Namibian Constitution⁴, which states:

- “1. 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.
2. Searches of the person or the homes of individuals shall only be justified:
 - (a) where these are authorised by a competent judicial officer;
 - (b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.”

It could be argued that this constitutional provision is clear and crisp, but its scope has never been meaningfully defined by a court of law, although current regulatory developments around mandatory SIM card registration have opened up room for litigation against the backdrop of Article 1⁵3.

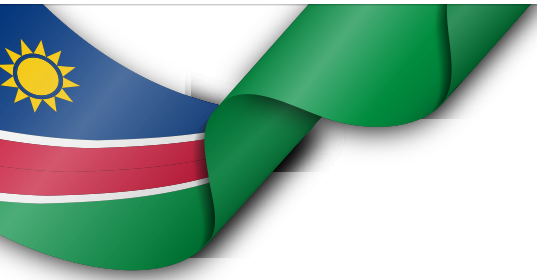
While Namibia has not yet enacted a law protecting online privacy and personal data, the country’s National Cybersecurity Strategy and Awareness Raising Plan 2022 – 2027⁵ posits privacy and personal data protection as critical priorities to ensuring cybersecurity. The strategy, in the foreword, expresses the recognition that its aims include protecting Namibian “netizens’ privacy”. In fact, Pillar 1 of the six strategic pillars is “Privacy and Personal Data Protection”, which states that eventual data protection legislation will be in line with international standards.

Furthermore, the strategy states that one of its three guiding principles is “Fundamental Human Rights”, with its design based on “respect for universally agreed fundamental rights, including, but not limited to, the United Nations’ Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, as well as relevant multilateral or regional legal frameworks”.

3 <https://action-namibia.org/government-seeks-public-input-on-draft-data-protection-bill/>

4 <https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf>

5 <https://drive.google.com/file/d/1Zh2B1qpzLiLo80LttqN0fbvhJb-zW1TNq/view?usp=sharing>



In this regard, it states that in its rollout “attention should be paid to freedom of expression, privacy of communications and personal-data protection”.

However, while the above statements are very consequential, it should be noted that the strategy does not incorporate a human rights framing in its higher-level statements, such as the mission and vision.

Aside from these domestic and international frameworks informing the country’s attempts at legislating around online privacy and data protection, at a regional level, Namibia is one of the few African countries that has ratified the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention)⁶.

Despite these frameworks and instruments supposedly informing the drafting of the latest version of the online privacy and data protection bill of October 2022, the bill appears to considerably fall short of the human rights standards emanating from these frameworks and instruments.

The 2020 draft vs the 2022 draft

As indicated earlier, in October 2022 input and comments were suddenly invited by MICT on a draft data protection bill and it quickly became clear that the bill in question differed markedly with one that was shared for comment in late 2020.

An analysis of the October 2022 draft, compiled by the South Africa-based ALT Advisory on behalf of the Institute for Public Policy Research (IPPR) and the Access to Information in Namibia (ACTION) Coalition⁷, found the differences between the two versions of the bill highly problematic in many respects.

The analysis report⁸, which was submitted to MICT ahead of the 31 October 2022 deadline, starts off by stating that “we note that the present iteration of the Bill (as circulated in October 2022 and dated 2021) appears to be substantially different in comparison to previous versions of the Bill, particularly the draft 2020 version of the Bill which was subject to a multi-stakeholder engagement in February 2020”.

The report goes on to state: “The present iteration of the Bill is of concern and, in multiple instances, removes or amends necessary and important sections from the 2020 version of the Bill, including, among others ... Part III of the 2020 Bill which affirms the rights of data subjects.”

And it continues: “While the reason for these sweeping changes remains unclear, they are addressed, in part, in these submissions. However, as a result of these changes, the Bill should be further developed following this public participation process and further opportunities to provide written submissions on future versions of the Bill should be provided to all stakeholders, including civil society.”

Human rights concerns

Some of the areas of specific human rights concern raised about the 2022 draft were underdeveloped consent provisions, the almost complete absence of protections for data subjects, and the absence of carve-outs for journalistic, artistic and academic data collection and processing.

With regard to consent provisions, the civil society analysis states: “Adding the element of prior consent to all data subjects strengthens the definition of “consent” in section 1 of the Bill and ensures that data subjects must consent to the processing of their personal data prior to processing.”

As for issue of the protection of the rights of data subjects, the civil society submission calls for reintroduction of “Part III of the 2020 version of the Bill as a new Part 2 in the present Bill, with the “Data Protection Supervisory Authority” part becoming a new Part 3. This will correctly give prominence to the primary rights holders in the Bill: data subjects.” Part III of the 2020 version lays out comprehensive protections for data subjects, which were completely absent from the latest draft.

6 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

7 <https://action-namibia.org/https-action-namibia-org-wp-content/uploads-2022-11-action-data-protection-submission-pdf/>

8 <https://action-namibia.org/wp-content/uploads/2022/11/ACTION-Data-Protection-Submission.pdf>

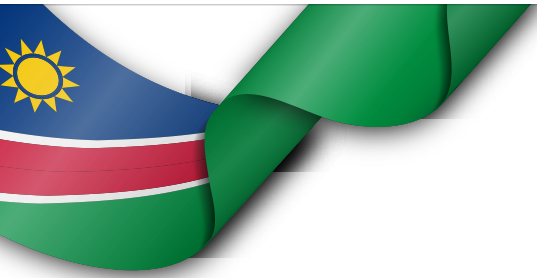


Photo credit: Shutterstock

In terms of freedom of expression concerns around the lack of recognition of the significance of provisioning for journalistic, artistic and academic data collection and processing, the civil society report states: “An express exemption for journalistic, literary, or artistic purposes should be recognised in the Bill, either in section 34(1) (f) or section 43, and should provide that “The Act does not apply to the processing of personal data solely for the purpose of journalistic, literary, or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression, including press freedom.” (Additionally, an express exemption for processing personal data for academic purposes, with sufficient safeguards, should be considered by MICT.)”

Conclusion

It is against the backdrop of these, and a host of other, shortcomings of the draft privacy and data protection bill that civil society concluded that in its present form, the Bill is not fit for purpose and called for further consultations.

At the time of finalising this article such consultations were scheduled to take place through March 2023 in communities across the country under the auspices of the Ministry of ICT. It was hoped that these consultations would address the identified shortcomings and weaknesses in the bill towards addressing “the inherent need to protect and promote the rights of data subjects in Namibia”. ■

Unregulated CCTV in Zambia sparks data privacy concerns



M W A Z I
S A K A L A



M A U R E E N
M U L E N G A

Zambia Drafts Legislation to Regulate CCTV for Privacy and National Security.

As Zambia continues to embrace technology on its quest to promote the Smart Cities Initiative, several pieces of legislation have been drafted including the Closed Circuit Television Public Protection Bill of 2021. This comes in the wake of increased use of technology in the public service and the integration of information technology in the provision of services in the public and private sector.

Closed Circuit TV (CCTV) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. CCTV relies on strategic placement of cameras, and observation of the camera's input on monitors remotely.

In Zambia, CCTV is increasingly being used by individuals in private spaces as a means of security to either monitor premises or provide a deterrent to would be criminals. They have also been deployed alongside road infrastructure as a component of remote road traffic management and speed monitoring.

Such public use of CCTV is able to identify and record additional data apart from just video. The use of CCTV for face recognition or tracking of motor vehicles based on their number plate registration has raised the important question about a person's right to privacy and as such a suitable legislation is required to ensure Zambia falls within the universally accepted parameters.

Background

Zambia adopted a Smart City initiative in 2015, implemented in three phases. The first step in this initiative is establishing a national cloud data centre. The second is installing a national broadband network. The third involves building cloud platforms in a smart grid.

The government through then Chief Government Spokesperson Dora Siliya said that they had decided to introduce a bill on CCTV because there was no legal framework to regulate the use of CCTV in private and public premises in the country despite the fact that the technology is becoming affordable and has been widely used.

In the absence of appropriate safeguards, data and CCTV acquire a distinct sensitivity and vulnerability, as compared with paper documents, to risks arising from available means of unauthorised access, use, misappropriation, alteration, and destruction.

Zambia, as a party to several international charters, endeavours to domesticate international and regional agreements with the Zambia Law Development Commission (ZLDC), a statutory body created under Chapter 32 of the laws of Zambia, primarily mandated to implement law reform.

In the ZLDC report¹ submitted to the Minister of Home Affairs and Internal Security, the Zambia Law Development Commission chairperson Mrs. Justice Roydah Kaoma said the use of Closed-Circuit Television (CCTV) has gained high importance in numerous sectors due to its efficiency and working benefits.

Legal landscape

Zambia currently lacks a legal framework regulating the use of CCTV. There's a noticeable rise in individuals and businesses adopting CCTV systems without any governing regulations. This situation poses potential threats to both national security and individual privacy.

Numerous countries have effectively implemented public surveillance systems, aiding in crime reduction and offender prosecution. Law enforcement agencies globally utilize CCTV footage from private installations in their investigations. Encouraging and supporting the installation of CCTV in private spaces accessible to the public and in public areas across Zambia is crucial. However, this should be accompanied by a comprehensive legal framework. Such regulations are imperative to prevent abuse, safeguard privacy, and uphold national security standards.

The Ministry of Home Affairs and Internal Security engaged the Zambia Law Development Commission (ZLDC) to develop a legislative framework which ensures clarity and certainty in the use of CCTV and which also provides for uniformity of rights and obligations and redress where arising rights and duties are violated.

On Monday 17 June 2019, at the Cabinet Meeting at State House the introduction of a Bill that would regulate the use of Closed-Circuit Television (CCTV) in private and public premises was approved². According to a report published in the Zambia Daily Mail newspaper on 18 June 2019, then Minister of Information and Broadcasting Services Dora Siliya, who was Government Chief spokesperson, disclosed that there had not been sufficient legislation in place to regulate the use of such technology.

According to a Montreal AI Ethics report³ submitted by Sarah Chiumbu, not only are civilians unaware of such practices, but they also are not encouraged to be informed. Chiumbu notes that Zambian civilians would see CCTV cameras being erected but not know their purpose. There was no public consultation on the Smart City initiative the CCTV cameras facilitate. Even if there was a consultation, surveillance technology would need to be expressed in accessible language rather than general political jargon.

The Convention on the Organisation for Economic Co-operation and Development (OECD) urged Governments, the public sector and the private sector to take steps to protect information systems and to provide for their security, and established Guidelines for the Security of Information Systems in 1992.⁴ These guidelines were replaced by the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security and again in 2015 by the OECD's high level recommendations on Digital Security Risk Management for Economic and Social Prosperity.⁵

The Universal Declaration on Human Rights⁶, as agreed to by member states which include Zambia, pledges to achieve the promotion of universal respect for and observance of human rights and fundamental freedoms.

-
- 1 REPORT ON CLOSED-CIRCUIT TELEVISION PUBLIC PROTECTION BILL, 2021 – Zambia Law Development Commission
 - 2 CABINET NODS CCTV BILL ~ (zNBC.co.zm)
 - 3 <https://montrealaiethics.ai/reports-on-communication-surveillance-in-botswana-malawi-and-the-drc-and-the-chinese-digital-infrastructure-surveillance-in-zambia/>
 - 4 Recommendation of the Council of the OECD concerning guidelines for the security of information systems 26 November 1992: <https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm>
 - 5 OECD Guidelines for the Security of Information Systems and Networks / Lignes directrices de l'OCDE r.gissant la s.curit. des syst. mes et r.seaux d'information
 - 6 [udhr_booklet_en_web.pdf \(un.org\)](#)



Photo credit: 2M Assets

The Declaration is not legally binding, however, it forms part of customary international law, and has been the basis of the development of numerous human rights treaties.

Article 5 provides “No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment”. Article 15 of the Constitution of Zambia is premised on this provision. The right to protection from inhumane and degrading treatment is one of the four non-derogable rights. If the use of covert cameras is to be allowed in the development of the proposed legislation, this should be done in a manner which does not result in degrading treatment particularly to data subjects such as prisoners in correctional facilities. In addition, where covert cameras are to be used, they must comply with principles and standards set out in this instrument.

Article 7 stipulates that, “All are equal before the law and are entitled without any discrimination to equal protection of the law”. Therefore, all human beings are entitled to equal protection against any discrimination in violation of the Declaration and against any incitement to such discrimination.

Article 12 provides that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. This section speaks to Article 17 of our Constitution, which protects the right to privacy, however, this may be derogated from if it is in public interest.

Article 20 provides that “everyone has the right to freedom of peaceful assembly and association”.

If the use of mobile surveillance cameras at public gatherings, among others, is to be provided for in the proposed law, this is to be done in a manner which does not hinder the aforementioned right, and such provision must have safeguards, such as limitations on the period of time such footage may be kept by law enforcement officers.

All Member States are required to ensure all of the aforementioned provisions are brought into fruition as stipulated in Article 28 which reads “Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.”

In a situation where Government authorities are conducting surveillance of an individual, they could easily harvest data from systems outside of their mandate by tapping into footage of street cameras, hospital facilities or even private shopping areas.

The African Charter on Human and Peoples’ Rights⁷ (also known as the Banjul Charter) is an international human rights instrument that is intended to promote and protect human rights and basic freedoms in the African continent. Zambia is a party to this instrument and has since ratified it.

Article 1 of the Banjul Charter provides that “The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Chapter and shall undertake to adopt legislative or other measures to give effect to them”.

7 36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf (au.int)

This article speaks to Article 13 and 18 of the Constitution of Zambia which provides for protection of the rights to personal liberty and secure protection of the law respectively.

Further the Africa Union Charter on Cyber Security and Personal Data Protection⁸ provides a guideline for establishing a credible framework for personal data protection in Africa through the protection of personal data and e-governance among others.

Conclusion

As Zambia has continued to roll out various technology centred pieces of legislation, the capacity to implement these has been brought into question, especially in view of some conflicting clauses in terms of enforcement or regulation.

CCTV is commonplace in many shops and there are no guidelines on storage of data or even consideration of individuals' privacy.

Love of Home shop manager Liyah Chabala shared that CCTV has been very helpful in the management of stock at the shop, because they were able to detect suspicious behaviour and even capture footage of thefts which protected the store from losses.

However, when asked if the use of CCTV in the shop should be regulated, it was her opinion that in the same way a Trade Licence was issued, trade entities should also be compelled to have CCTV because it would help in monitoring activities and providing evidence in case of wrongdoing or false reporting.

A customer, who opted to remain anonymous shared how the CCTV footage was helpful because it helped resolve an issue she had faced when she had discovered that an item she had paid for, was not packed.

It would appear that the use of CCTV has been embraced as a norm and the adoption of regulation would easily be assimilated. However, the capacity to monitor or even back up data garnered from public and private CCTV systems remains in doubt.

As technology continues to advance and artificial intelligence begins to be the main engine behind systems, it opens up the possibility of illegal surveillance being undertaken based on face recognition technology or personal identification that could be seen as a breach of privacy and an encroachment on personal rights. ■

References

1. Legislation as a tool for the Use of Public Security Information Systems in Zambia article published by the Zambia Law Development Commission authored by In'tutu Akolwa. <http://www.zambialawdevelopment.org/legislation-as-a-tool-for-the-safe-use-of-public-security-information-system-in-zambia/>
2. <https://www.znbc.co.zm/news/cabinet-nods-cctv-bill/>
3. <https://www.parliament.uk/globalassets/documents/post/pn175.pdf>
4. <https://montreal.ethics.ai/reports-on-communication-surveillance-in-botswana-malawi-and-the-drc-and-the-chinese-digital-infrastructure-surveillance-in-zambia/>
5. <https://www.znbc.co.zm/news/govt-adopting-tech-to-protect-citizens/>
6. REPORT ON CLOSED-CIRCUIT TELEVISION PUBLIC PROTECTION BILL, 2021 – Zambia Law Development Commission
7. <https://montreal.ethics.ai/reports-on-communication-surveillance-in-botswana-malawi-and-the-drc-and-the-chinese-digital-infrastructure-surveillance-in-zambia/>
8. Recommendation of the Council of the OECD concerning guidelines for the security of information systems 26 November 1992 (<https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm>)
9. OECD Guidelines for the Security of Information Systems and Networks / Lignes directrices de l'OCDE r.gissant la s.curit. des syst. mes et r.seaux d'information
10. udhr_booklet_en_web.pdf (un.org)
11. 36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf (au.int)
12. 29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)

8 29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)



Photo credit: Memory Mangombe, The Herald

Zimbabwe's digital leap falls short in bridging access to justice gaps



N O M P I L O S I M A N J E

Zimbabwe Judiciary's Digital Transformation Faces Challenges in Access and Security.

T rue to the digital era that we are living in, several stakeholders have been going digital as was noted mostly during the COVID 19 pandemic, with increased uptake of internet banking, online news and e-government strategy among others. This also included the digitisation of the education sector in Zimbabwe through the implementation of the national e-learning strategy.

The judiciary has also not been left behind as strides have already been made towards going digital. On the occasion of the official opening of the 2022 Legal Year on the 10th of January 2022 under the theme, "Use of technology to enhance efficiency and the rule of law in the judiciary" Chief Justice Luke Malaba noted the following,

"The Judiciary appears to have been slow in adopting electronic justice as it has found comfort in traditional ways of doing things, such as reliance on hard copies of books, allowing of physical appearances in courts, and the filing of physical documents.

1 <https://www.zimbabwesituation.com/news/digital-learning-to-cover-all-schools/>



The Judiciary is doing this at its own peril, as the use of information communication technology has increasingly become the normal way of doing any business, including the business of delivering justice.”

In light of the above agenda, on the 1st of May 2022, the Judicial Service Commission in Zimbabwe officially launched the Integrated Electronic Case Management System (IECMS) and also the first paperless court in Zimbabwe - the Commercial Court Division of the High Court. The first phase of the implementation of the IECMS focuses on the Constitutional Court, Supreme Court and the Commercial Court Division of the High Court, while the other courts will be integrated in the second phase.

In February 2023, the Labour Court and also the Administrative Court also started utilising the IECMS, as part of the second phase.² It is reported that some litigants had challenges using the system allegedly due to network challenges.

The IECMS integrates systems from other stakeholders or institutions within the judicial sector which include the Zimbabwe Republic Police, the National Prosecuting Authority, the Zimbabwe Prisons and Correctional Services and judicial officers.³

This system facilitates digital access to judgements, online case tracking, virtual court hearings, e-filing of cases and e-payment of fees among other features. The launch of this system thus brings to the fore a plethora of internet governance issues.

Internet governance issues with regards to the IECMS

Access to devices

To begin with, access to devices like a laptop, computer or smart phone is a key requirement for the use of this system. In September 2021, the Zimbabwe National Statistics Agency-ZIMSTATS and the Postal and Telecommunications Regulatory Authority of Zimbabwe presented a report on ICT Access by Households and Individuals which highlighted that 58.8% of Zimbabwean households have a smart phone. Of the aforementioned percentage, the majority of the smart phone owners are based in urban areas. This shows the limited access to smart phones in Zimbabwe and more so the continued exclusion of people in rural and marginalised communities.

A March 2022 report indicated a much lower smart phone penetration rate at 52% while 22 % of the devices were reported to have low data handling capacity.⁴

Despite the aforementioned, in November 2021, the finance minister Mthuli Ncube proposed a USD\$50.00 levy on all mobile phones to curb tax evasion, and such levy would be collected prior to registration of new cellular handsets by mobile network operators, thus further restricting access to devices.

2 <https://www.synisys.com/news/labour-and-administrative-courts-in-zimbabwe-go-digital/#:~:text=The%20second%20phase%20was%20built,High%20Court%20of%20the%20country.>

3 http://www.jsc.org.zw/jscbackend/upload/Speech/Presentation%20eCase_ZIMIECMS_30%20March%202022.pdf

4 <https://www.paynow.co.zw/blog/smartphone-penetration-rate-in-zimbabwe/>



"The Judiciary appears to have been slow in adopting electronic justice as it has found comfort in traditional ways of doing things, such as reliance on hard copies of books, allowing of physical appearances in courts, and the filing of physical documents." - Chief Justice Luke Malaba.

Digital literacy

Further, for one to interact on the system and enjoy its benefits or features, they need to create an account by registering on the website.⁵ The system will require that one enters their personal details like full name, country code, cell phone number, email address, username and password. An activation email is then sent to the person's email address to activate the account and from there on, access to the system is by logging in using the username and password.⁶

Based on the aforementioned, digital literacy emerges as another pivotal factor. All previously mentioned stakeholders should possess the capability to use smart devices, navigate the internet proficiently, create email accounts, and access the IECMS platform. This proficiency in digital literacy is essential not only for legal practitioners filing cases online and attending virtual hearings but also for self-represented individuals. Additionally, judges require digital literacy as they draft orders and judgments.

One group that has been normally left behind in technological advances is the elderly. There is a definite need to provide digital literacy trainings which is in line with the 2022 theme for the World Telecommunications and Information Society Day, "Digital technologies for older persons and healthy ageing".

In the build up to and post the launch of the IECMS, the Law Society of Zimbabwe and the Judicial Service Commission provided trainings for legal practitioners to familiarise and understand the system. However, more work needs to be done particularly to equip other stakeholders and broadly the public.

Access to the internet

As noted in the above description of how the IECMS works, it is clear that one needs quality internet access in order to be able to use the system. This is restricted, however, due to high costs of data and also limited infrastructure.

The Q3 2021 POTRAZ Sector Performance report showed that internet penetration in Zimbabwe stood at 62.6%⁷ while the 2022 report by Data Reportal, indicated an even lower penetration rate of 30.6 % of the total population.⁸

The recently published Q4 2022 Sector Performance Report by POTRAZ showed a 14,9% decline in mobile data usage and also an increase in operating costs for the players in the telecommunications industry.⁹

5 <https://zimiecms.org.zw/login>

6 Obey Manyenga, A new dawn as Zim Court go digital, Zim Juris, Issue 1, 2022

7 <https://www.techzim.co.zw/2021/12/internet-penetration-active-mobile-subscriptions-more-from-the-potraz-q3-2021-report/>

8 <https://datareportal.com/reports/digital-2022-zimbabwe>

9 <https://www.techzim.co.zw/2022/07/declining-data-usage-spiraling-operating-costs-telcos-not-sitting-pretty/>



A culture of cybersecurity

Court processes involve filing documents that contain personally identifying information, such as names and service addresses. Moreover, when establishing an IECMS account, individuals are required to provide personal information. Given that this system integrates multiple stakeholders within the judicial sector, cybersecurity becomes exceptionally critical.

In Zimbabwe, several cases have been reported where government websites have been hacked including the Ministry of Defence, the National University of Science and Technology, and zoom meetings of government agencies. While one of the requirements when setting up the account is a security question and answer which can be relied on for recovering passwords or account should the user forget, more strides should be made towards promoting a culture of cybersecurity for both institutions and individuals.

Conclusion

The digitisation of Zimbabwe's judiciary marks a significant stride in the nation's digital transformation. However, there's an immediate need for cross-sector collaboration to ensure that this advancement doesn't restrict access to justice. The civil society sector, POTRAZ, Ministry of ICTs, and the Judicial Service Commission bear the responsibility of enhancing access to smart devices, affordable and reliable internet, digital literacy, as well as ensuring digital safety and security. Such a system is crucial for fostering justice, and it's imperative that members of the public are not left behind. Therefore, concerted and collaborative efforts must be undertaken to ensure comprehensive public awareness. ■

References

1. <https://www.zimbabwesituation.com/news/digital-learning-to-cover-all-schools/>
2. <https://www.synisys.com/news/labour-and-administrative-courts-in-zimbabwe-go-digital/#:~:text=The%20second%20phase%20was%20built,High%20Court%20of%20the%20country.>
3. http://www.jsc.org.zw/jscbackend/upload/Speech/Presentation%20eCase_ZIMIECMS_30%20March%202022.pdf
4. <https://www.paynow.co.zw/blog/smartphone-penetration-rate-in-zimbabwe/>
5. <https://zimiecms.org.zw/login>
6. Obey Manyenga, A new dawn as Zim Court go digital, Zim Juris, Issue 1, 2022
7. <https://www.techzim.co.zw/2021/12/internet-penetration-active-mobile-subscriptions-more-from-the-potraz-q3-2021-report/>
8. <https://datareportal.com/reports/digital-2022-zimbabwe>
9. <https://www.techzim.co.zw/2022/07/declining-data-usage-spiraling-operating-costs-telcos-not-sitting-pretty/>

digital rights

SOUTHERN AFRICA

