PARADIGM INITIATIVE

Digital Policy Digest

No. 3 of 2024

An Analysis of the Zimbabwean Cyber and Data Protection Regulations, 2024

Privacy Under Surveillance: Namibia's SIM Card Registration and Biometric Data Collection

Public Participation in Zimbabwe's AI Policy making process

Evaluating Ethiopia's Hate Speech and Disinformation Prevention and Suppression Proclamation

Digital Policy Digest

No. 3 of 2024

This Digital Policy Digest (DPD) documents digital rights policies and laws and presents guidance on areas needing reform. This edition assesses and features an analysis of the Zimbabwean Cyber and Data Protection Regulations, 2024, Namibia's SIM Card Registration and Biometric Data Collection, an assessment of Public Participation in Zimbabwe's AI Policy making process an evaluation of the Hate Speech and Disinformation Prevention and Suppression Proclamation in Ethiopia.

This publication is not for sale. It is provided as a part of Paradigm Initiatives mission to "Connect African youth with digital opportunities and ensuring digital rights for all". The Digital Policy Digest is published quaterly by Paradigm Initiative.

Researchers: Thobekile Matimbe, Jessica Uiras, Bridgette Ndlovu, and Selamawit Tezera Chaka. **Editorial Designer:** David Chima

An Analysis of the Zimbabwean Cyber and Data Protection Regulations, 2024

This article looks at the implications of the Zimbabwean Cyber and Data Protection Regulations, 2024 on privacy.

By Thobekile Matimbe

01

Introduction

Undisputedly, the data protection regulations are necessary for the full operationalisation of the Cyber and Data Protection Act [Chapter 12:07],(CDPA) in compliance with section 32 of the CDPA. However, it is important that regulations promote and not pose a threat to human rights. The government of Zimbabwe promulgated the Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024[1] (the Regulations) on 13 September 2024. The CDPA prescribed in section 32 the passing of regulations ensuring that there is compliance with the protection of personal data. The CDPA's objective is to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.

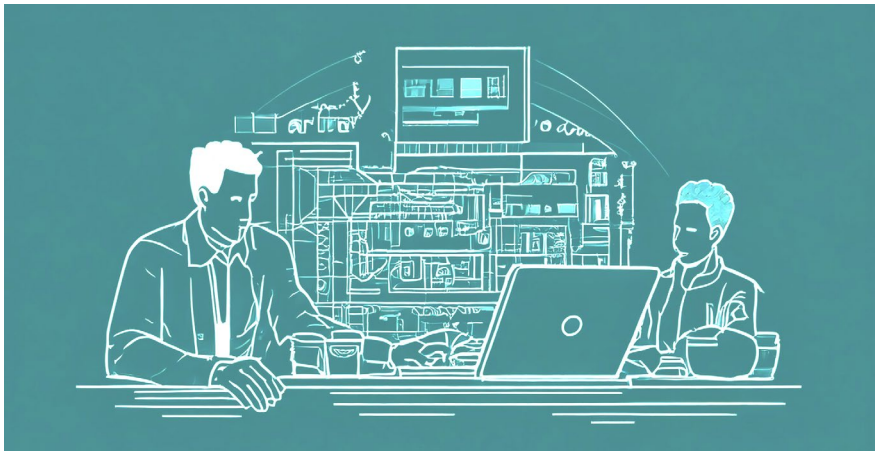
When the CDPA was initially passed in December 2021 as the Data Protection Act[2], it's objective focused on increasing data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects . The title and object were then amended through a republication on 11 March 2022 to be read as the Cyber and Data Protection Act. Notably, the change in objective potentially signals a shift from prioritisation of protecting personal data to build confidence and trust, to prioritising targeted mass communications surveillance 'in the name of' addressing cyber security. The implementation of the CDPA and Regulations should address this risk by ensuring that privacy, a right entrenched in section 57 of the Constitution of Zimbabwe Amendment (No.20), 2013[3] is protected.

1. https://www.veritaszim.net/node/7187
2. https://www.veritaszim.net/sites/veritas_d/files/Data%20Protection%20Act%205%20of%202021.pdf
3. https://www.veritaszim.net/node/315

Positive Aspects

The Regulations contain provisions that ensure the protection of personal data, calling on data controllers to notify the regulatory authority - Postal & Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) of any data breaches within 24 hours and ensuring the protection of children's rights to data privacy, among others. They also call for data controllers to appoint data protection officers (DPOs), which is a progressive step towards a culture of data privacy in Zimbabwe. The Regulations also give a 6-month timeline to data controllers to appoint DPOs and be licensed which is important in the data governance chain. The Act stipulates that all data controllers must report a breach within 24 hours to the regulatory authority. The CDPA defines a data controller as any natural person or legal person who is licensable by the Authority and includes public bodies and any other person who determines the purpose and means of processing data in terms of section 3 of the Act.

> The regulation calls for data controllers to appoint data protection officers (DPOs), which is a progressive step towards a culture of data privacy in Zimbabwe.



Notable Concerns

Data Breaches

While section 17(1) of the Regulations provides that a data controller shall report personal data breaches to the Authority within 24 hours of becoming aware of the breach, there is no general direction to also notify the data subject of the breach. A data subject is defined by the CDPA as an individual who is an identifiable person and the subject of data. Personal data belongs to data subjects and they should be notified as well. However, the Regulations stipulate that only where a detected breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, should the data subject be notified within 72 hours. Drawing best practices from other countries, section 22(1)(a) of the South African Protection of Personal Information Act[4] and section 49(3) of the Zambian Data Protection Act[5] provide for general notification of data subjects where there is a data breach. This promotes transparency by data controllers to victims of data breaches.

Implications on Instant Messaging Platforms

The Regulations provides as follows:

3. (1) No person shall process personal information for the purposes indicated in subsection (2) unless they are licensed with the Authority.

(2) Subject to section 4, any person who processes personal information with the intention to—(a) decide the means, purpose or outcome of the processing; (b) decide what personal data should be collected; (c) decide which individuals to collect

4. https://www.gov.za/sites/default/files/gcis_docu201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf
5. https://www.parliament.gov.zm/node/8853

personal data from; (d) obtain a commercial gain or other benefit from the processing of personal data; shall apply for a licence in terms of these regulations.

(3) of the Regulations, any person who processes personal information without a data controller licence within the stipulated time frames shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

The CDPA provides for the protection of personal data and within this context, aims to ensure that before personal data is processed, there is informed consent and that data controllers do not abuse the consent to violate rights such as privacy by sharing personal data with third parties. This means that data controllers should ensure that they process data only in line with the purposes for which data is collected, giving individuals protection as well as agency over the use of their personal data. The requirement of licensing ensures that data controllers adhere to good data protection practices and comply with the CDPA. However, section 3(2)(d) should not be wrongfully understood to suggest that messaging platforms like WhatsApp should be monitored by the government or that WhatsApp administrators should obtain licences based on their general role as WhatsApp administrators for personal and household activity.

> Data controllers should ensure that they process data only in line with the purposes for which data is collected

Challenges with Enforcement on WhatsApp Administrators

The WhatsApp platform being an instant messaging platform makes it a difficult task to monitor based on human rights considerations.

- Monitoring WhatsApp to enforce the Regulations against perceived data controllers suggests violating encryption, digital surveillance and seizure of digital tools.
- WhatsApp users have a level of agency over what they share and can delete within specific timelines based on the security features in the WhatsApp application.
- WhatsApp group managers can moderate the group by ensuring terms of engagement are adhered to.
- Where conflict arises in WhatsApp groups the group administrators can remove a member.
- Aggrieved members can remove themselves from WhatsApp groups.

Digital surveillance of messaging platforms is a threat to human rights and should not be promoted.To strengthen user agency over data shared online,the government should implement digital security awareness and sensitisation activities. This approach empowers data subjects to have agency over their data and to demand accountability where their privacy is breached.

Data Protection and Instant Messaging Platforms

Where an instant messaging platform administrator processes personal data for commercial reasons or any other benefit, as envisaged by the CDPA and Regulations, then an administrator of an instant messaging platform may fall within the definition of a data controller. The CDPA defines processing of personal data in the text box below:

> "processing" refers to any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data, including—
>
> a. organisation, adaptation or alteration of the data;
> b. retrieval, consultation or use of the data; or
> c. alignment, combination, blocking, erasure or destruction of the data;

Where a data controller processes data and leaks information to a messaging platform like WhatsApp, website or platform like Facebook as witnessed during COVID-19, they commit a data breach and should be held accountable for breaching privacy. In 2020, cases of data breaches were noted in Zimbabwe, including COVID-19 Case No.15: A Zimbabwean victim of misinformation recorded in the COVID-19 and Digital Rights: A Compendium on Health Surveillance Stories in Africa[6]. Any business or government entity that uses messaging platforms to leak personal data should be held accountable in terms of the CDPA and the Regulations. This also suggests the need to assess whether or not they are data controllers in terms of the CDPA before calling upon them to be licensed in terms of section 3 of the Regulations. The Regulations should not be misunderstood to suggest a general designation of WhatsApp group administrators as data controllers.

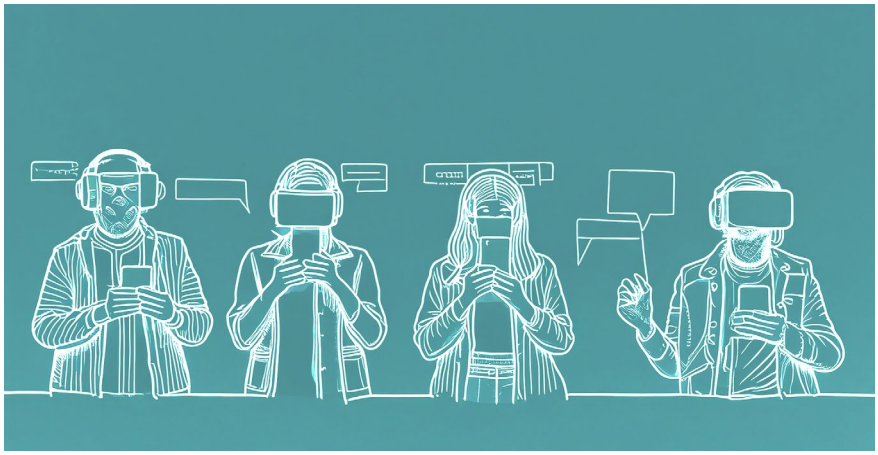
Broad Provision

Section 3(2)(d) of the Regulations is an overly broad provision that states that any person who processes personal information for commercial gain or any other benefit is liable. The 'any other benefit' component makes the provision subject to misinterpretation and misuse targeting groups such as researchers, the media and human rights defenders. This impact is an inherent consequence of any law that has broad provisions. Laws and regulations should have clarity to help individuals to comply, according to the principle of legality[7]. This provision suggests that anyone who processes data for not only commercial reasons but any other benefit would be liable and could mean anything or be interpreted anyhow by law enforcement agents. This problematic aspect requires clarity for avoidance of doubt.

WhatsApp[8] is an example of an instant messaging platform that has end-to-end encryption built within its system to ensure privacy of communications. Policing WhatsApp administrators or other instant messaging platform ad-

6. https://paradigmhq.org/report/covid-19-and-digital-rights-a-compendium-on-health-surveillance-stories-in-africa/
7. https://ideas.repec.org/p/smo/jpaper/044dg.html
8. https://faq.whatsapp.com/820124435853543

ministrators is digital surveillance[9] that poses a threat to privacy, freedom of expression and association.It has to be provided for by a law and also be a legitimate restriction on the right to privacy. Enforcement of such measures would be achieved through a witch hunting exercise that does more harm than good. The way this may be enforced is through a violation of human rights to secure evidence to warrant any enforcement measure.



Protecting Encryption and Privacy of Communications

A major concern is that enforcing the Regulations on instant messaging platform administrators would potentially enable targeted mass communications surveillance, violations of encryption safeguards, ordering internet intermediaries to monitor content they did not generate and seizure of digital technologies. The ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019[10] (the Declaration) provides in Principle 39(2) that States shall not require internet intermediaries to proactively monitor content which they have not authored or otherwise modified. Principle 40(2) provides that everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies. Principle 40(3) highlights that laws should not weaken

9. https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/surveillance/#:~:text=Government%2Dled%20digital%20surveillance,past%2C%20present%2C%20or%20future.
10. https://achpr.au.int/en/node/902

> A major concern is that enforcing the Regulations on instant messaging platform administrators would potentially enable targeted mass communications surveillance, violations of encryption safeguards, ordering internet intermediaries to monitor content they did not generate and seizure of digital technologies.

encryption, unless such measures are justifiable and compatible with international human rights law and standards.

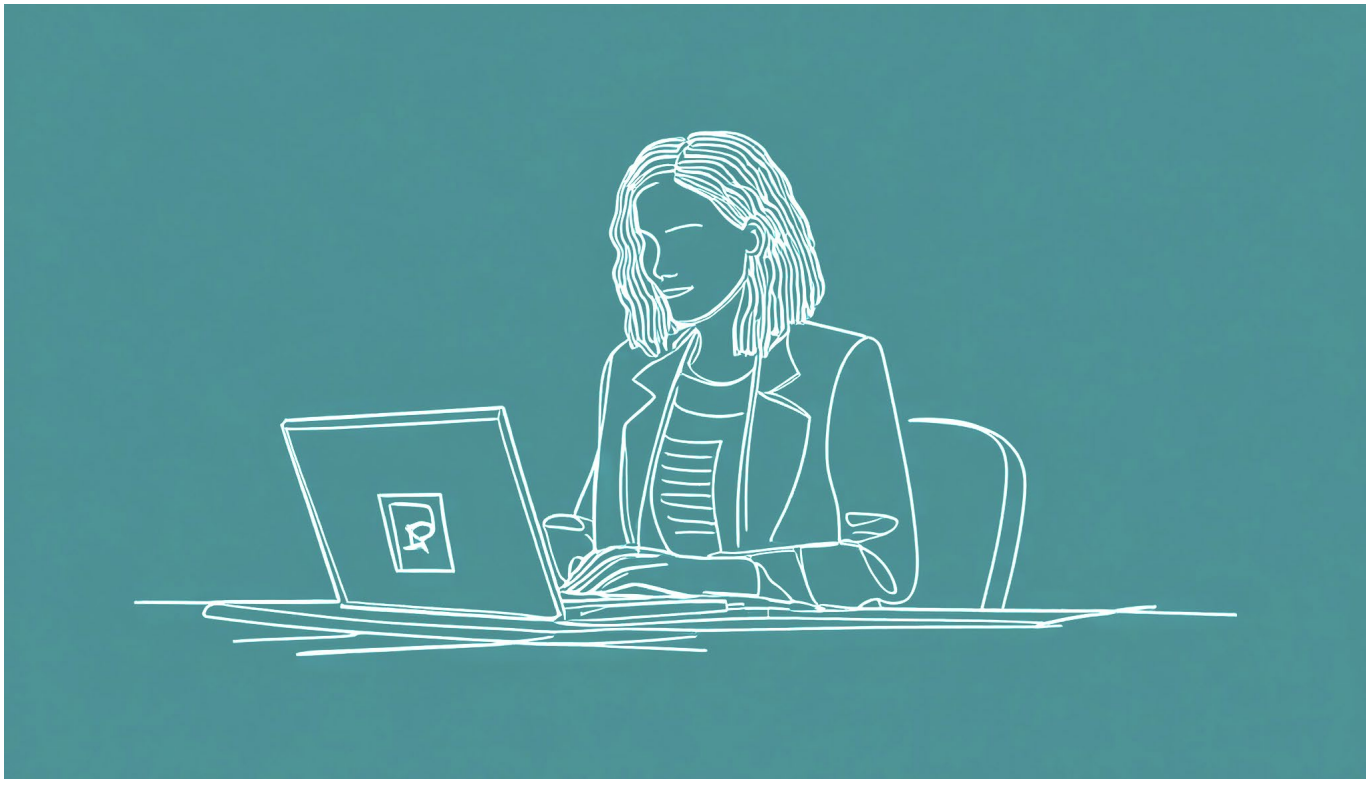
The Declaration stipulates in Principle 41(1) that States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications. Principle 41(3) provides that States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including being subject to judicial oversight and due process. The Declaration, in this regard, echoes the importance of ensuring that communication platforms are safeguarded in the promotion of privacy.

The ACHPR also passed Resolution 573 on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa[11] in November 2023 where it called on African States to 'promote and encourage the use of privacy-enhancing technologies and desist from adopting laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards.' The government must not enact broad laws that threaten the use of privacy-enhancing platforms and violate encryption.

11. https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication

Conclusion

The Regulations are a commendable step towards fostering data protection in Zimbabwe. However, they should discard any broad implications. They should be interpreted and implemented in the spirit of safeguarding personal data and not as a threat to freedom of expression. Privacy of communications should be promoted by ensuring that instant messaging platform administrators do not become targets for State orchestrated digital surveillance. Guidelines to enforcement of the Regulations by the POTRAZ can help clarify the extent to which privacy of communications are safeguarded and targeted digital surveillance avoided.



Privacy Under Surveillance: Namibia's SIM Card Registration and Biometric Data Collection

By Jessica Uiras

02

Introduction

Namibia's mandatory SIM card registration, established under the Communications Act of 2009[12], was passed to combat identity fraud, enhance national security, and align the country with global telecommunications practices. However, this law has extended into biometric data collection without comprehensive protections, raising significant privacy concerns. Mobile Telecommunication company (MTC), Namibia's primary telecom provider, now requires citizens to submit fingerprints and facial scans to activate SIM cards, leaving Namibians vulnerable to state surveillance and potential misuse without the security of a dedicated data protection law. The rolling out of sim card registration is happening outside of a data protection law to protect personal data collected through sim card registration and biometric data collection. This article explores the implications of SIM registration and biometric collection, emphasising the urgent need for stronger data governance policies that align with Namibia's constitutional and human rights obligations.

12. https://www.npc.gov.na/wp-content/uploads/2022/06/Communication-Act.pdf

SIM Registration as a State Surveillance Tool

Government's Justification for SIM Registration

The Namibian government justifies mandatory SIM card registration as a critical tool for enhancing national security and combating cybercrime. Part 6 of the Communications Act of 2009, titled "Interception and Monitoring of Telecommunications," provides the legal framework for this policy. It mandates that telecommunications providers collect and retain user information for up to five years, enabling the identification of users and the lawful interception of communications under judicial authority. These measures aim to deter criminal activities such as identity theft and fraud.

The Regulations in Terms of Part 6 of Chapter V of the Communications Act, 2009, gazetted in Government Gazette No. 7481 on 15 March 2021[13], further enforce the requirements for SIM registration. These regulations obligate service providers to collect detailed customer information, including full names, addresses, and identification numbers, as part of the registration process.

During the launch of the SIM Registration Awareness Campaign, former ICT Minister Dr Peya Mushelenga highlighted that this policy aligns Namibia with over 157 countries implementing similar measures, ensuring compliance with international standards. The policy was also framed as vital for facilitating e-commerce, digital identity, and crime prevention strategies.

While these regulations are positioned as necessary for national security, critics highlight the lack of safeguards to protect citizens' privacy. The broad powers granted under Part 6 of the Act, including data retention and interception,

13. Communications Act 8 of 2009 - Regulations 2021-040

risk infringing on constitutional rights, particularly in the absence of a comprehensive data protection framework to oversee the use and storage of such sensitive information.

zExtended Data Retention and Privacy Risks

Under Section 73 of Namibia's Communications Act of 2009, telecommunications providers are required to collect and retain extensive customer information, including call records, metadata, and other transactional details, for a period of five years. This data retention policy facilitates the identification of telecommunications users and supports law enforcement efforts, particularly in investigating and prosecuting criminal activities. However, the lack of clear data handling standards and oversight mechanisms leaves this sensitive information vulnerable to misuse, abuse, and security breaches.

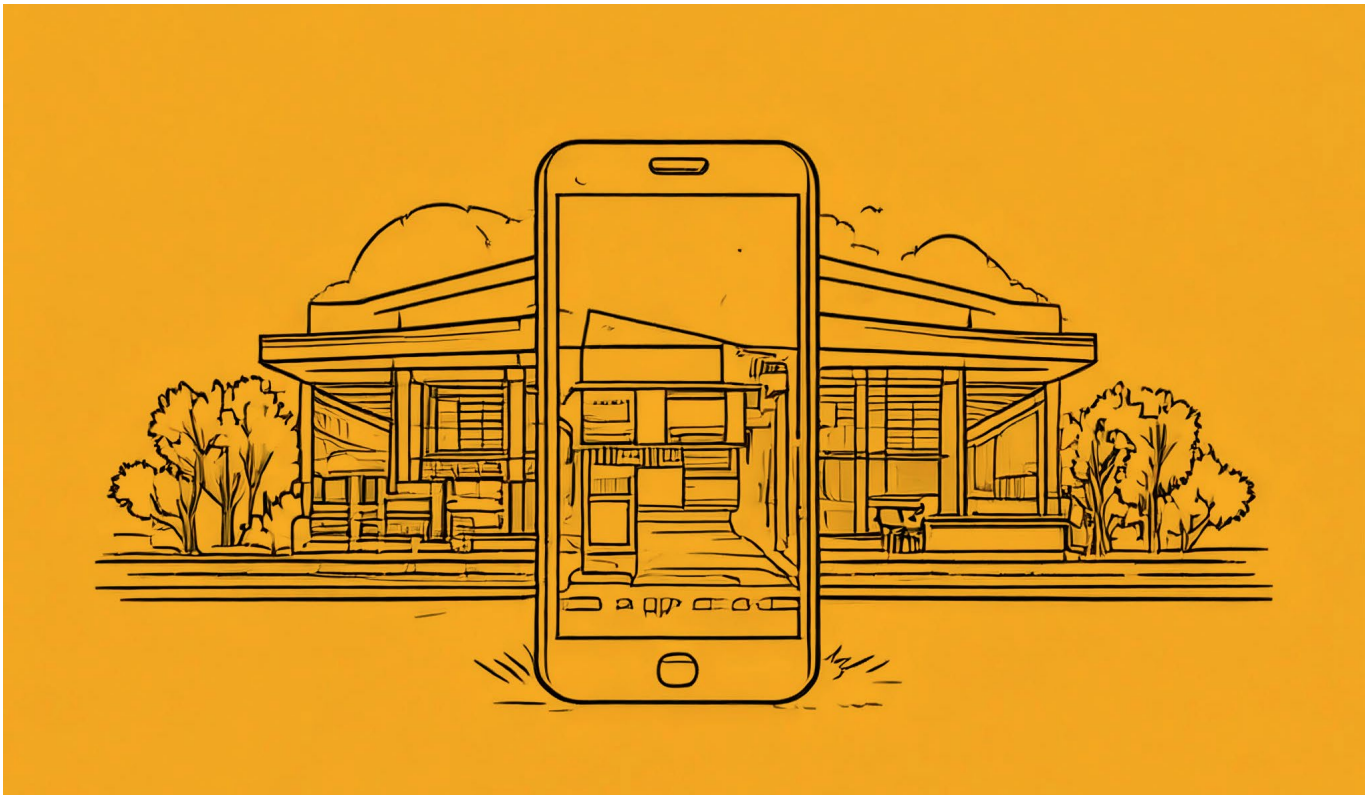
The practice of long-term data retention creates an environment ripe for mass surveillance, as it enables the government and authorised agencies to monitor individuals' communications and activities over extended periods. While intended to bolster national security, such measures inherently erode personal freedoms by undermining privacy rights and discouraging free expression.

> The practice of long-term data retention creates an environment ripe for mass surveillance, as it enables the government and authorised agencies to monitor individuals' communications and activities over extended periods.

Without a comprehensive data protection law, there are no established safeguards to prevent the misuse of

this retained data or to hold institutions accountable for breaches. This absence not only threatens the confidentiality of private communications but also exacerbates power imbalances, where the state has far-reaching surveillance capabilities with little to no checks in place. For citizens, this means living under the shadow of potential overreach, where every communication is traceable and permanently recorded, irrespective of its relevance to national security.

A better approach would be to implement data minimization principles, retaining only essential data for limited timeframes, and establishing strict accountability and oversight mechanisms to protect individual freedoms while addressing security needs.



Biometric Data Collection and Privacy Risks

1. MTC's Mandatory Biometric Collection

Although Namibia's Communications Act does not explicitly require biometric data collection for SIM registration, MTC implemented its Verifi system[14], mandating the submission of fingerprints and facial scans for all customers. This requirement stems from MTC's 31 January 2023 press release[15], which declared Verifi as a mandatory condition for accessing all MTC services. The rationale provided includes combating identity fraud and enhancing the security of SIM registration processes, a measure framed in alignment with the draft Namibian Data Protection Bill and international standards such as the GDPR and the AU Convention on Cybersecurity and Personal Data Protection. However, no specific legislation supports MTC's mandatory biometric collection, raising concerns about the lack of legal safeguards for protecting such sensitive personal data

2. Lack of Legal Protections for Biometric Data

Namibia's failure to enact a comprehensive data protection law leaves a glaring gap in regulatory standards for managing biometric data. This legislative vacuum means entities like MTC are not held accountable for securely storing and responsibly using sensitive data. Biometric data, by its very nature, is particularly vulnerable because it is permanent and irreplaceable unlike passwords or other changeable identifiers. Without stringent safeguards, the unchecked collection and storage of biometric data

14. https://www.mtc.com.na/prepaid/verifi
15. https://www.mtc.com.na/uploads/press_releases/Press_release_-_Sim_reg_and_Virifi_Update.pdf

not only heighten the risk of breaches but also create a fertile ground for surveillance overreach and misuse.

The absence of enforceable legal frameworks undermines individuals' privacy and erodes public trust in digital governance. Robust data protection measures, including transparency in collection processes, clear limitations on data retention, and mechanisms for oversight, are urgently needed to ensure the responsible handling of such sensitive information. Until these safeguards are in place, biometric data collection in Namibia remains a significant privacy concern.

Implications for Human Rights and Constitutional Privacy

1. Lack of Compliance with Constitutional Protections for Digital Privacy

Article 13 of the Namibian Constitution[16] guarantees the right to privacy, explicitly protecting individuals from interference with their homes, correspondence, and communications except as prescribed by law and necessary in a democratic society for purposes such as national security or public safety. This provision can be interpreted to encompass digital privacy, placing a constitutional obligation on the state to protect personal data.

The absence of comprehensive data protection laws, however, undermines these constitutional guarantees. While

16. https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf

Article 13 provides a strong foundation, the lack of supporting legislation means that privacy rights are left unenforced in practice. For instance, the mandatory SIM card registration process requiring extensive data collection operates in a legal vacuum, leaving users without safeguards against potential misuse or abuse of their data. To comply with the Constitution, Namibia must urgently enact data protection laws that establish clear guidelines on data collection, retention, and use, ensuring compliance with privacy rights guaranteed under Article 13.

2. Chilling Effect on Expression and Confidentiality

Namibia's SIM card registration requirements[17], combined with the absence of robust data security measures, pose significant risks to freedom of expression and confidentiality. Part 6, Chapter V of the Communications Act of 2009 mandates that telecom providers retain customer data for up to five years, allowing agencies such as the Namibia Central Intelligence Service (NCIS) to request this data under judicial authorisation. This raises concerns about excessive surveillance, particularly given the lack of transparency in how this data is managed or accessed.

Such a surveillance environment fosters self-censorship, as individuals may refrain from expressing dissenting views or engaging in sensitive communications for fear of being monitored. This chilling effect undermines the democratic principles of free expression. Furthermore, inadequate safeguards for data management also jeopardise the confidentiality required in sensitive professions like journalism, law, and healthcare, where breaches could have serious implications for vulnerable groups.

To mitigate these risks, Namibia must implement oversight mechanisms for data collection and retention, ensuring that access to such data is limited, transparent, and compliant with constitutional and human rights standards.

17. https://mtc.com.na/sim/sim-registration-en

Conclusion

Namibia has ratified the Malabo Convention[18] and aims to align with frameworks like the GDPR[19], yet without domestication and enforcement, these standards remain a fiction. Countries like South Africa have set strong precedents by implementing data protection laws[20], limiting biometric data use and ensuring transparency. Namibia could model similar protections to curb surveillance abuses and build public trust in its digital systems. Namibia's SIM card registration and biometric data collection policies, implemented without comprehensive data protection laws, expose citizens to privacy violations and unchecked surveillance. Passing the Data Protection Bill[21] is crucial to safeguard Namibians' rights and align with international standards. Establishing privacy-centred policies will enable Namibia to secure a balanced digital environment that respects individual freedoms and promotes trust. As such it is recommended that the government enacts a data protection law that protects the right to privacy in line with the Namibia Constitution.

18. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
19. General Data Protection Regulation (GDPR) – Legal Text
20. https://popia.co.za
21. Namibia advances data protection and cybercrime legislation amid rising cyber threats - Innovation Village | Technology, Product Reviews, Business

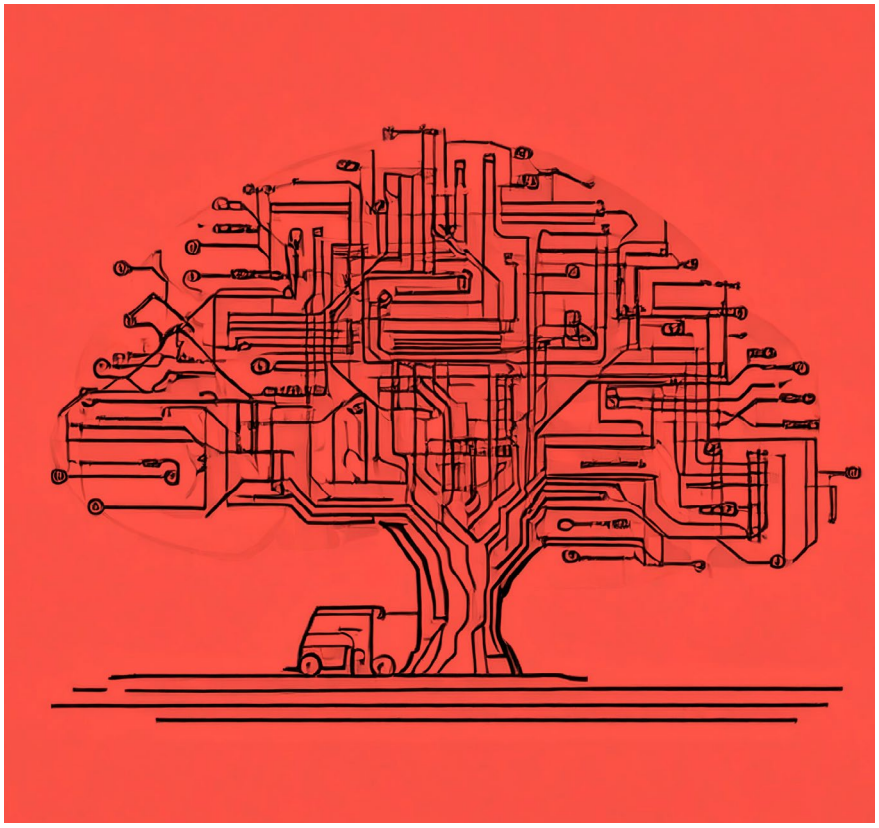
Public Participation in Zimbabwe's AI Policy making process

By Bridgette Ndlovu

03

Background

The Zimbabwean government has completed the process of developing a national Artificial Intelligence (AI) policy aimed at regulating the use of AI and related technologies across various sectors. This initiative was highlighted by the Minister of Information Communication Technology, Postal and Courier Services, Tatenda Mavetera[22]. The initiative is progressive as it is a step towards ensuring the ethical use, security, and the promotion of AI technologies in the country. The AI policy will aid Zimbabwe to harness the potential of artificial intelligence for national development. However, despite announcements of the completion of the policy, it is not publicly available for scrutiny and there have been no open calls for public participation in the development of the policy raising concerns of exclusion of key stakeholders in the development of the AI policy. As such, this analysis points at best practices without direct reference to the alleged Zimbabwean AI policy.



22. https://www.herald.co.zw/national-ai-policy-framework-complete/#:~:text=The%20national%20artificial%20intelligence%20policy,and%20improve%20ordinary%20people's%20livelihoods.

AI Regulation and Zimbabwe's involvement regionally and globally

Artificial Intelligence (AI) offers transformative benefits but also presents risks. To manage the potential risks, governments and regional bodies must develop norms and regulations that govern the use of AI. Recently, the African Union passed the Continental AI Strategy[23] during its 45th Ordinary Session in Accra, Ghana, on July 18-19, 2024. The strategy underscores the continent's commitment to a development-focused approach to AI and aims to be a guiding document for countries that are in the process of developing their AI policies. The strategy seeks to promote ethical, responsible, and equitable practices across the continent.

In Africa, countries such as Rwanda, Benin, Egypt, Morocco, Mauritius, Tunisia, Sierra Leone, Senegal and Nigeria are leading the race as they have developed National AI policies to govern the use of AI. The policies highlight research and development in AI, construction of robust data infrastructures, skills development, development of local AI solutions, increasing AI funding and investment incentives, and providing secure and trusted African data as priorities.

It is worth noting that in 2023, the United Nations Scientific and Cultural Organisation (UNESCO) announced that Zimbabwe is one of the 50 countries engaged with UNESCO on the Recommendation on the Ethics of AI[24], which guide the implementation of the Readiness Assessment Methodology (RAM)[25]. UNESCO's Recommendation on the Ethics of AI is a global normative framework that guides

23. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy
24. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence
25. https://www.unesco.org/en/articles/unesco-support-more-50-countries-designing-ethical-ai-policy-year

AI's ethical development and use and is operationalised through the RAM. UNESCO developed the RAM in 2022 as a tool for assessing a country's legal, social, cultural, scientific, educational, technical and infrastructural AI capacities. The tool also indicates whether a country's AI systems align with the values, principles and policy areas in UNESCO's Recommendation. Zimbabwe's participation in the RAM process is an important milestone in developing AI Policy.

Zimbabwe is involved in multilateral discussions on lethal autonomous weapons systems (LAWS). In November this year, Zimbabwe voted[25] in favour of the draft resolution L.77 on Lethal and Autonomous Weapon Systems (LAWS)[26], which was adopted by the First Committee of the United Nations General Assembly (UNGA) on November 5, 2024. The resolution reflects states' apprehensions about the potential negative implications of LAWS on global security, ethical considerations and regional stability. The Resolution emphasises maintaining human control over decisions involving lethal force. It asserts that algorithms should not have full control over decisions that can result in killing or harming humans, underscoring the need for accountability in military operations. The resolution was adopted with 161 states voting in favour, 3 against, and 13 abstentions, demonstrating broad support for addressing the challenges posed by autonomous weapons.

Public Participation in Policy Making

Public participation in policymaking is a crucial aspect of democratic governance that calls for engaging citizens in decision-making processes that affect their lives. To improve the quality and legitimacy of policy decisions, it is

26. https://www.stopkillerrobots.org/news/161-states-vote-against-the-machine-at-the-un-general-assembly/
27. https://documents.un.org/doc/undoc/ltd/n24/305/45/pdf/n2430545.pdf

important for the Zimbabwean government and governments globally to engage citizens through public hearings and calls for input. This can enhance trust between citizens and the government and promote transparency and accountability in policy design.

To improve the quality and legitimacy of policy decisions, it is important for the Zimbabwean government and governments globally to engage citizens through public hearings and calls for input.

Zimbabwe needs to meet the expectations of UNESCO in the Multistakeholder AI Development: 10 Building Blocks for Inclusive Policy Design. The building blocks stem from three policy-making phases: agenda setting, drafting, implementation and evaluation. During the agenda-setting phase, governments should examine the scope of the national AI landscape, determine its strengths and weaknesses, gather knowledge and information and map stakeholders' needs, constraints, and influence.

According to the building blocks Zimbabwe should do the following:

- Raise awareness on the impact of AI on society
- Agree on a definition of AI and the terminology used during the policy process
- Establish an expert group to determine the national AI landscape. The Multistakeholder Expert Group (MEG) should be composed of policy and regulation authorities in ICT or digital economy as well as National Statistical offices and the AI and digital transformation related stakeholders, academic, technical community, private sector, journalists and media organisations, civil society, individual users of AI-based products and services, and any relevant intergovernmental groups. The MEG should also be cognisant of

gender, regional, ethnic and other dynamics.

- Outline the different stages in the multistakeholder AI policy process
- Develop the policy through open and inclusive consultations
- Commit to incorporating participants' feedback
- Make AI policy agile, flexible and responsive to evolving needs
- Develop AI policies based on Human Rights, Data Protection and Ethics Guidelines
- Combine the AI Strategy with an Action Plan
- Monitor and evaluate throughout the policy cycle

Conclusion

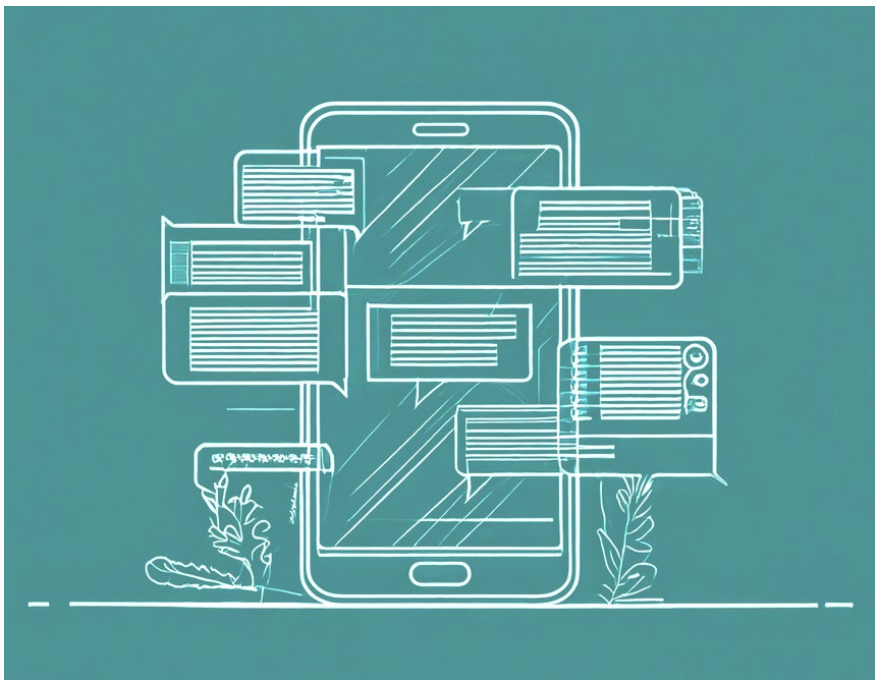
Zimbabwe 'jumped' to the second phase of the policy-making process by designing, reviewing and fine-tuning draft policy measures. When the document is eventually made publicly available, it will not have captured the needs of all stakeholders as public participation in line with the building blocks for inclusive policy design, was limited. Zimbabwe should adhere to international standards of effective policy making allowing all interested stakeholders to participate effectively in the process and develop representative policies that respect rights.

Evaluating Ethiopia's Hate Speech and Disinformation Prevention and Suppression Proclamation

By Selamawit Tezera Chaka

Introduction

Since 2018, Ethiopia has faced significant social and political challenges, exacerbated by the proliferation of hate speech and misinformation. These issues have intensified ethnic tensions, violence, and social unrest within the country. Addressing these harmful phenomena, particularly their online manifestations that lead to real-world harm, has been repeatedly highlighted as an urgent task by both state and non-state actors to mitigate violence facilitated by social media. One of the most debated pieces of legislation in Ethiopia in 2019 was the Hate Speech and Disinformation Law[28]. Despite concerns raised by local and international analysts, the Cabinet approved the law in November 2019, and the then President Sahle-Work Zewde gave her assent in March 2020. The internet rights organization, Access Now, underscored the negative implications of this law, warning that it could mark the beginning of a restrictive era for press freedom in Ethiopia unless revised.[29] This paper provides an in-depth analysis of the proclamation, examining its strengths, weaknesses, and offering recommendations for improvement.



28. Hate Speech and Disinformation Prevention and Suppression Proclamation No.1185 /2020
29. Access Now. (2020). Ethiopia's hate speech and disinformation law: The pros, the cons, and a mystery https://www.accessnow.org/ethiopias-hate-speech-and-disinformation-law-the-pros-the-cons-and-a-mystery/

Best Parts of the Proclamation

The proclamation demonstrates the government's commitment to addressing the destructive impact of hate speech and misinformation in the country. Several aspects of the law are commendable. Primarily, the proclamation includes preventive measures to create a safer and more inclusive environment by regulating harmful content and promoting responsible speech. The law, in article 5 s (5) and (6), mandates public awareness campaigns to educate citizens about the dangers of hate speech and misinformation, thus fostering a more informed populace[30]. This responsibility is mainly given to the Ethiopian Broadcasting Authority and Ethiopian Human Rights Commission. It also encourages collaboration between government agencies, media outlets, and civil society organizations to combat these issues. Moreover, the law provides mechanisms for rapid response and corrective actions to prevent the spread of harmful content. This proactive stance is a significant strength of the proclamation, as it allows for timely intervention and resolution of issues before they cause widespread harm.

Drawbacks of the Proclamation

From the start, civil society actors have given recommendations to the several drawbacks in the proclamation in regards to its effectiveness and potential misuse.

30. Hate Speech and Disinformation Prevention and Suppression Proclamation

One of the primary issues with the proclamation is the broad definition of "hate speech" and "misinformation", which can lead to potential misuse and suppression of legitimate expression and dissent. This ambiguity makes it challenging to distinguish between harmful speech and protected free speech. This will possibly lead to the possible overreach and unintended consequences. Additionally, the imposition of criminal sanctions for publishing, disseminating, or possessing content deemed as hate speech or misinformation can stifle free expression and discourage critical discourse. The threat of severe penalties may result in self-censorship, with individuals and organizations avoiding the discussion of controversial topics for fear of reprisal. This chilling effect undermines the fundamental right to freedom of expression and hampers the open exchange of ideas essential for a healthy democratic society.[31]

This ambiguity makes it challenging to distinguish between harmful speech and protected free speech. This will possibly lead to the possible overreach and unintended consequences.

Furthermore, the lack of clarity in implementation procedures can lead to inconsistencies and potential injustices, as the enforcement mechanisms are not well-defined, resulting in arbitrary application of the law. This lack of transparency and consistency can erode public trust in the legal framework and its ability to effectively address the issues it seeks to combat. Lastly, the proclamation can have a chilling effect on the media, as journalists and news organizations may practice self-censorship to avoid falling foul of the law. This law can have far-reaching consequences on media freedom, as it undermines the role of the press in providing accurate information and facilitating informed public discourse.[32]

31. Access Now. (2020). Ethiopia's hate speech and disinformation law: The pros, the cons, and a mystery https://www.accessnow.org/ethiopias-hate-speech-and-disinformation-law-the-pros-the-cons-and-a-mystery
32. The Reporter Ethiopia. (2020). Ethiopia's new hate speech and disinformation law: An analysis. https://www.thereporterethiopia.com/9053/

Recommendations for Improvement

To enhance the effectiveness and fairness of the proclamation, several recommendations can be proposed. First, the definitions of "hate speech" and "misinformation" should be refined to be more precise to avoid overreach and ensure clarity. Clear and specific criteria should be established to distinguish between harmful content and protected speech. Second, the proclamation should be aligned with international human rights standards to ensure that it does not infringe on freedom of expression[33]. It is possible to amend this law as per ACHPR Declaration Principle 22 (2) where States shall repeal laws that criminalize sedition, insult, and publication of false news[34]. Thus, by adopting internationally recognized principles, Ethiopia can balance the need to prevent harm with the protection of individual rights. This alignment will also enhance the credibility and legitimacy of the legal framework.

Additionally, though major government institutions were given the responsibility of public education campaign, there is a gap as both institutions are not effectively doing it. Thus, collaborating with civil society actors is critical in enhancing public education regarding harmful contents. Also, encouraging a culture of critical thinking and media literacy will empower individuals to identify and counter harmful content, reducing its impact. Investing in capacity-building initiatives for law enforcement and judicial personnel is also essential to ensure consistent and fair application of the law. Finally, implementing a mechanism for the regular review and revision of the law will address emerging challenges and ensure its continued relevance and effectiveness. This mechanism should include periodic assessments of the law's impact and the incorporation of feedback from stakeholders. This continuous refining of the legal framework can give a chance to adapt to the evolving nature of hate speech and misinformation and ensure that its response remains effective and just.

33. Access Now. (2020). Guide: How to protect human rights in content governance. https://www.accessnow.org/guide-how-to-protect-human-rights-in-content-governance/
34. African Commission on Human and Peoples' Rights (2019), Declaration of principles on freedom of expression and access to information in Africa: file:///C:/Users/hp/Downloads/declarationofprinciplesonfreedomofexpressioneng2019.pdf

More About PIN

Paradigm Initiative has worked in communities across Nigeria since 2007 and across Africa since 2017, building experience, community trust, and an organisational culture that positions us as a leading non-governmental organisation in ICT for Development and Digital Rights on the continent. Across our regional offices in Kenya, Nigeria, Senegal, Zambia, Zimbabwe, Cameroon, the Democratic Republic of Congo (DRC), and beyond, we have impacted youth with improved livelihoods through our digital inclusion and digital rights programs. The organisation's programs include Life Skills. ICTs. Financial Readiness. Entrepreneurship (LIFE) Training Program, a digital readiness workshop for girls, and Life@School Club Program. PIN has also built online platforms that educate and serve as safe spaces for reporting digital rights violations. These mediums, in the form of reports, short films, and educational online platforms, include Ayeta, Londa, and Ripoti. The organisation is also the convener of the annual Digital Rights and Inclusion Forum (DRIF), a pan-African platform where conversations on digital policy in Africa are shaped, policy directions debated, and partnerships forged for action. The forum has been held since 2013.

PARADIGM INITIATIVE

Free download of this policy digest and past issues, visit www.paradigmhq.org or scan code: