MISA ZIMBABWE

POLICY BRIEF

Addressing The Gaps In The Data Protection, Privacy And Surveillance Legislation

Prepared by Nkosana Maphosa & Innocent Mandongwe

Addressing The Gaps In The Data Protection, Privacy And Surveillance Legislation

Published By

Media Institute for Southern Africa
www.misa.org

Design & Layout

OnaDsgn
hello@onadsgn.com
www.onadsgn.com

ISBN: 9781779065353

Contents

Executive Summary 4

Background 5

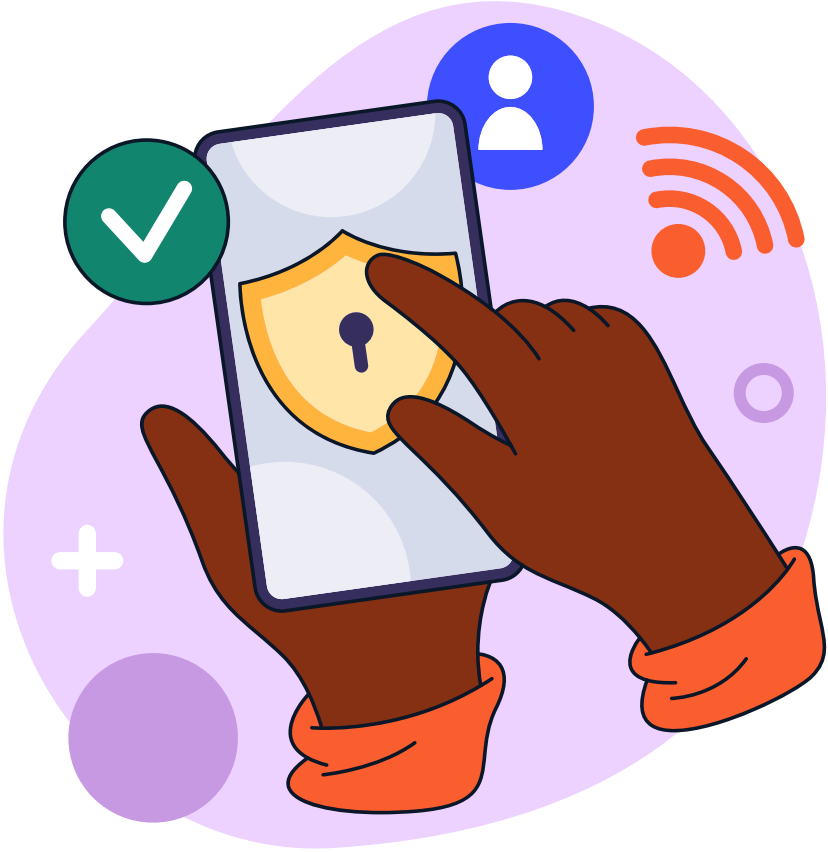
Data Protection And Privacy Legislation 7

Recommendations 14

Conclusion 17

References 18

1. Executive Summary



Zimbabwe has various pieces of legislation that affect data protection, privacy, and surveillance.[1] The relevant pieces of legislation regarding data protection and privacy include, but are not limited to, the Cyber and Data Protection Act [Chapter 12:07] and the Postal and Telecommunications Act [Chapter 12:05].
The main relevant pieces of legislation regarding surveillance are the Interception of Communications Act [Chapter 11:20] and the Postal and Telecommunications Act. The supposed principal purpose of these pieces of legislation is to give effect to various fundamental rights and freedoms enshrined in the Constitution of Zimbabwe Amendment (No.20) Act, 2013, including the right to privacy, freedom of expression, and access to information[2].

1. See also, Section 21 of the Freedom of Information Act [Chapter 10:33]; s 15 of the Postal and Telecommunications (Internet Services) Regulations (Statutory Instrument 262 of 2001); the Postal and Telecommunications (Subscriber Registration) Regulations (Statutory Instrument 95 of 2014); the Banking Amendment Act No.12 of 2015; Section 48 of the Consumer Protection Act [Chapter 14:44]; National Registration Act [Chapter 10:17]; Census and Statistics Act [Chapter 10:05]; National Social Security Authority Act [Chapter17:04]; Courts and Adjudicating Authorities (Publicity Restriction) Act [Chapter 7:04].
2. See Sections 57, 61 and 62 of the Constitution.

The adequacy of the pieces mentioned above of legislation in giving full effect to the relevant constitutional rights can be assessed by reference to the best international standards[3]. The international standards are captured and set out in various instruments, including the Southern African [4]Development Community (SADC) Model Law on Data Protection, the African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention),[5] Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019,[6] the International Principles on the Application of Huma Rights to Communications Surveillance and the European Union (EU*)* General Data Protection Regulations (GDPR). In that regard, it is imperative to point out that the Cyber and Data Protection Act, the main legislation dealing with data protection and privacy in Zimbabwe, is mainly modelled on the EU GDPR, as it borrows the bulk of its provisions. Accordingly, it is appropriate to use the EU GDPR as the main benchmark for assessing the adequacy of the provisions of the Cyber and Data Protection Act concerning data protection and privacy.

This policy brief posits that there are various yawning gaps in our data protection, privacy and surveillance legislation. The gaps include but are not limited to, the absence of independent data protection and cyber monitoring authorities, the limited scope of data subject rights, an inadequate framework for cross-border data transfers, a draconian surveillance regime and a lack of effective remedies against data and privacy breaches. Accordingly, this policy brief recommends a litany of measures to plug and bridge the gaps to achieve a legal framework that fully reflects the underlying constitutional rights.

2. Background

As noted above, we have two main pieces of legislation that provide for surveillance in Zimbabwe. The major justification for surveillance laws is crime prevention, detection and investigation. The first piece of legislation is the Postal and Telecommunications Act. In terms of Section 98 of the said Act, a postal or telecommunication licensee or employee of such licensee in charge of a telegraph office is allowed to intercept or detain any telegram which he suspects of having contents that provide evidence of the commission of a criminal offence or of being sent to assist the commission of a crime; or upon request by a commissioned police officer who suspects it of having contents that provide evidence of the commission of a criminal offence or of being sent to assist the commission of a crime.

The second and main piece of legislation is the Interception of Communications Act. In terms of Section 6 of the said Act, authorised persons, who are defined to include the Chief of Defence Intelligence, the Commissioner of the Zimbabwe Republic Police (“*ZRP*”) and the Commissioner General of the Zimbabwe Revenue Authority (ZIMRA) or their nominees, are allowed to intercept any communication upon issuance of a warrant by the Minister of Transport and Communications. In that regard, postal and telecommunication service providers are required in Section 9 of the Interception of Communication Act to ensure that their postal or telecommunications systems can technically always support lawful interceptions. In 2014, the

3. A holistic, contextual and purposeful reading of the law supports this. See, for example, Sections 34, 46 (1) (c) & (e), 326, 327 of the Constitution and the International Treaties Act [Chapter 3:05]. Several cases have confirmed the import of international standards at the domestic level.
4. Core human rights instruments such as the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights and the African Charter on Human and Peoples’ Rights etcetera are relevant here.
5. Zimbabwe is not a signatory to the Malabo Convention as yet. This instrument was adopted on 27 June 2014 by the Twenty-Third Ordinary Session of the Assembly in Malabo, Equatorial Guinea.
6. https://achpr.au.int/en/node/902. See Principles 37-42 for example.

former Minister of State for National Security between 2005 and 2009, namely Didymus Mutasa, made a chilling statement to the effect that the government "*sees everything ... We have our means of seeing things these days, we just see things through our system. So, no one can hide from us in this country*"[7]. This statement is significant in that it suggests that the current surveillance powers reposed in the government are prone to abuse and weaponisation to the detriment of the constitutional right to privacy.

Accordingly, the fact that the surveillance powers set out in the Interception of Communications Act are apt to be abused implies gaps in the current state of surveillance legislation that warrant close examination.

As to data protection and privacy legislation, although the Cyber and Data Protection Act is the main relevant law, it is imperative to point out that in Zimbabwe, various pieces of legislation also have a bearing on data protection and privacy. For instance, regarding the Census and Statistics Act [*Chapter 10:29*], the use and disclosure of aggregate information collected and relating to commercial, agricultural, mining, social and general activities of inhabitants of Zimbabwe during a census is regulated and restricted. Further, under the Consumer Protection Act [*Chapter 14:44*], disclosing any customer's confidential information is prohibited[8].

In addition, in terms of Section 7 (1) (d) of the Electoral (Voter Registration) Regulations, 2017 Statutory Instrument 85 of 2017, a person's biometric features are captured during voter registration. Further, in terms of Sections 4 and 5 of the Postal and Telecommunications (Subscriber Registration) Regulations, 2014 Statutory Instrument 95 of 2014, telecommunication service providers are required to obtain, record and store a customer's information and details before SIM-card registration.

In terms of Section 8 (1) of the said Regulations, customer's information obtained and recorded by a telecommunication service provider is stored in the so-called Central Subscriber Information Database. Section 8 (2) (c) of the Regulations provides that the purpose of the Central Subscriber Information Database is, *inter alia*, to enable the Postal and Telecommunications Regulation Authority ("*POTRAZ*") to assist law enforcement agencies or safeguard national security.

Further, Section 8 (5) of the Regulations states that the customer information in the Central Subscriber Information Database is held strictly confidential, and no persons or entities are allowed access to the information except authorised personnel. However, the Regulations do not expressly define the persons who qualify as authorised personnel.

Ahead of the 2018 and 2023 harmonised elections, many mobile phone users received unsolicited text messages from the Presidential candidate of the Zimbabwe African National Union-Patriotic Front (Zanu PF) canvassing for votes. It is not immediately clear how the third party managed to access the mobile phone users' personal data, such as their phone numbers. However, what is clear is that such data breaches suggest the existence of gaps in our data protection and privacy laws, which need to be addressed.

7. Newzimbabwe.com "CIO watching your bedrooms, Mutasa warns critics", ***New Zimbabwe*** 10 June 2014.
8. See section 78 of the Consumer Protection Act [***Chapter 14:44***].

3. Data Protection and Privacy Legislation

The Cyber and Protection Act is the main act that deals with data protection in Zimbabwe to give effect to the constitutional right to privacy. This can be gleaned from its long title, which states that the purpose of the Act is "*to provide for data protection with due regard to the Declaration of Rights under the Constitution*". It is submitted that, in terms of international best practices, the Cyber and Protection Act is blighted with various gaps that detract from its ability to properly and adequately provide for data protection and privacy.

3.1. Definitions

The Cyber and Data Protection Act laudably distinguishes between ordinary data and sensitive data for purposes of data protection. While the definition of sensitive data in Section 2 is quite broad, it does not encompass biometric data. Although the reference to biometric data in Section 12 of the Act suggests that biometric data is intended to enjoy the same high level of protection as sensitive data, it is submitted that it is imperative that, for the avoidance of data, the definition of sensitive data in Section 2 be amended to cover biometric data expressly. This is particularly necessary because there is wide processing of biometric data in our country. For instance, as noted above, in terms of Statutory Instrument 85 of 2017, a person's biometric data is captured for voter registration purposes.

Further, while Section 12 of the Act refers to biometric data, the term is not defined in Section 2. Accordingly, a definition of biometric data is needed in the Act to avoid doubt as to its envisaged meaning. In that regard, guidance as to the meaning of biometric data may be derived from Article 4 (14) of EU GDPR[9].
Further, while Section 2 of the Cyber and Data Protection Act defines data controller by inclusion of the term "licensable", there is no provision in the Act which sets out the criteria that a data controller must satisfy for it to be licensable. Accordingly, there is a need for a substantive provision in the Act which fleshes out the term licensable used therein. This is particularly important so that a data controller knows whether it is licensable, regulates its conduct and arranges its affairs accordingly.

3.2. Application of the Act

Section 4 (1) of the Cyber and Data Protection Act refers to the Protection of Personal Information Act [Chapter 10:27], which does not exist in our statute book. It stands to reason that such a reference requires removal to eliminate the confusion created thereby. Further, while the EU GDPR[10] and the Malabo Convention[11] expressly provide that they do not apply to the processing of personal data by a natural person during a purely personal or household activity, Section 4 of the Act does not stipulate such an exemption. It is submitted that the regulation of how a natural person handles their personal data during a purely personal or household activity constitutes an unwarranted intrusion upon the right to privacy. So, the Act should expressly state that it does not apply to such a situation to avoid doubt.

9. It defines biometric data as "personal data resulting from specific technical processing relating to the physical, physio logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".
10. See Article 2 (2) thereof.
11. See Article 9 thereof.

3.3. Designation of POTRAZ as the National Data Authority

Section 5 of the Act designates the Posts and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as the National Data Authority. It is submitted that such a designation is problematic in various material respects[12]. Firstly, since POTRAZ is also designated as the Cyber Security Centre and the regulator of the postal and telecommunications sector, its responsibilities are unwieldy and stretched thin, with the necessary corollary that its effectiveness and efficiency as a National Data Authority are likely to be compromised.

Secondly, since POTRAZ is subject to the Minister of Transport 16 and Communications policy direction and, the said Minister may direct the POTRAZ Board to reverse, suspend or rescind any decision or action,[13] POTRAZ is, arguably, not truly independent. In that regard, Article 52 (2) of the EU GDPR states that members of a national data authority must always be free from external influence, whether direct or indirect, and they must not receive instructions from anybody. In South Africa, there is the Information Regulator, which is subject only to the Constitution and to the law, and it is only accountable to Parliament[14]. It follows that POTRAZ does not pass the test of independence compatible with international best standards. Accordingly, there is a need to amend the Cyber Security and Data Protection Authority by establishing a separate and stand-alone National Data Authority, which is truly independent and not subject to the control of the Executive.

3.4. Principles relating to the processing of personal data

Section 13 of the Cyber and Data Protection Act sets out data controllers and processors' duties. However, these duties are essentially principles relating to the processing of personal data. They correspond to principles relating to processing personal data in Article 13 of the Malabo Convention and Article 5 of the EU GDPR. Conceptually, duties are different from principles. A duty is either a positive or negative obligation, but a principle is the value and spirit that must guide a person in performing the obligation. Accordingly, the so-called duties of data controllers and data processors under Section 13 of the Act must be correctly and expressly stated as principles relating to the processing of personal data.

Further, the scope of principles relating to the processing of personal data, as provided for in Section 13 of the Act, is not comprehensive. For instance, it omits the integrity and confidentiality principle in Article 5 (1) (f) of the UE GDPR.[15]. Accordingly, there is a need to broaden the scope of principles relating to the processing of personal data set out in the Cyber and Data Protection Act by incorporating the integrity and confidentiality principle therein.

12. Useful recommendations on Data Protection Authorities include the Privacy and Personal Data Protection in Africa-Advocacy Toolkit https://africaninternetrights.org/en/resource/privacy-and-personal-data-protection-africa-advocacy-toolkit which, we think should be examined in the Zimbabwean context.
13. See section 26 of the Postal and Telecommunications Act.
14. See section 39 of the Protection Personal Information Act No.4 of 2013.
15. It defines the integrity and confidentiality principle as processing personal data "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"

3.5. Rights of Data Subjects

Section 14 (a) of the Cyber and Data Protection Act enshrines the right to information of data subjects. However, it does not prescribe how the data controller should exercise the right. Accordingly, it is submitted that the right to information as provided for in Section 14 (a) should be enhanced by expressly imposing an obligation on the data controller to communicate the information to the data subject in a concise, transparent, intelligible and easily accessible manner; using clear and plain language.[16]

Further, the scope of the right to rectification enshrined in Section 14 (d) of the Act needs to be more comprehensive. It confines itself to correcting false or misleading information to the exclusion of completion of inadequate information. Accordingly, the scope of the right should be broadened to include the data subject's entitlement to completion of inadequate data, including the entitlement to provide a supplementary statement[17].

By the same token, the scope of the right to erasure (the right to be forgotten) enshrined in Section 14 (e) of the Act is not broad enough. It limits itself to the erasure of false or misleading personal information. It is submitted that the scope of the right to erasure should be broadened to include the erasure of all personal information, particularly where the personal information is no longer necessary in relation to the purpose for which it was collected; the data subject withdraws consent and the personal information has been unlawfully processed[18].

In addition, the right to object enshrined in Section 14 (c) of the Act should be enlarged to include the entitlement by the data subject to object at any time to the processing of personal data for direct marketing or campaigning[19] and to object to be subjected to a decision based solely on automated processing[20]. The express provision for the right to object to be subjected to a decision based solely on automated processing is particularly important considering the proliferation of artificial intelligence.

Further, the scope of data subject rights should be broadened by including additional rights. In that regard, there is a need to expressly enshrine the right to restriction of data processing in appropriate circumstances, including where the data subject contests the accuracy of the data; the processing is unlawful; the data controller no longer needs the personal information[21]. By the same token, there is need to enshrine the right to data portability expressly. Article 20 of the EU GDPR defines the right to data portability as the entitlement by a data subject "*to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided*".

In addition, a provision expressly requiring the data controllers to perform the obligations imposed on them by the data subject rights is needed.

16. See Article 12 (1) of the EU GDPR.
17. See Article 16 of the EU GDPR.
18. See Article 17 (1) of the EU GDPR.
19. See Article 21 (2) of the EU GDPR.
20. See Article 22 (1) of the EU GDPR.
21. See Article 18 of the EU GDPR.

3.6. Security Breach

Section 19 of the Cyber and Data Protection Act is too narrow in scope, and it accordingly fails to deal with the incident of data security breach adequately. For instance, it does not prescribe the minimum contents of the notification by the data controller to the National Data Authority in the event of a security breach.[22] Further, it does not oblige the data controller to notify the affected data subject of the personal data breach. This is particularly necessary and important where the breach of personal data is likely to result in a high risk to the rights and freedoms of natural persons[23]. Accordingly, Section 19 of the Act needs to be amended to address these deficiencies.

3.7. Obligations of Data Controllers

Section 22 of the Cyber and Data Protection Act implies that data controllers must seek specific authorisation from the National Data Authority regarding data processing, which poses specific risks to the fundamental rights of data subjects. It is submitted that Section 22 of the Act should be amended by imposing on the data controller an obligation to carry out a risk assessment as to the impact of the envisaged processing before the National Data Authority can grant the authorisation[24]. Further, it is submitted that there is a need for the Act to expressly impose on data controllers an obligation to have privacy policies in appropriate circumstances. In that regard, the Act should also prescribe the minimum content of such privacy policies to promote standardisation, harmonisation, and user-friendliness. For instance, the Act should require privacy policies to set out data subject rights and remedies clearly, concisely and simply.

By the same token, data controllers should be required to incorporate in their data policies or codes the obligation to carry out data protection by design and by default[25]. Data protection by design entails considering data protection risks while designing a new process, product or service rather than treating it as an afterthought. This involves assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure that processing complies with the Act and protects the rights of data subjects[26].

On the other hand, data protection by default entails having mechanisms to process only personal data necessary for each specific purpose. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary; and access is restricted to that necessary for each purpose.[27]

In addition, for transparency, accountability, and audit purposes, the Act needs to impose on data controllers an obligation to keep a detailed record of data processing activities, including the purpose of the processing, description of the categories of data subjects and personal data, and categories of the data recipients[28]. The obligation may be subject to the nature and size of the data controller.

22. See Article 33 (3) of the EU GDPR.
23. See Article 34 (2) of the EU GDPR.
24. See Articles 35 (1) of the EU GDPR.
25. See Section 25 of the EU GDPR.
26. See Data Protection Laws of the World at page 19
27. *Ibid.*
28. See Article 30 of the EU GDPR.

3.8. Cross-border data transfer

Section 28 (2) of the Cyber and Data Protection Act sets out the scope of considerations that a data controller must consider in assessing the adequacy of the level of protection afforded by a third party for cross-border data transfer. It is submitted that there is a need to broaden the scope of the said considerations by expressly including such factors as the rule of law, respect for human rights and fundamental freedoms, case law and effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred[29].

Further, the Act is silent on mechanisms of international cooperation concerning the enforcement of data subject rights arising out of cross-border data transfer. Accordingly, the Act should provide mutual legal assistance to multilateral and bilateral treaties[30]. The said mutual assistance processes and agreements should be documented, publicly available and subject to guarantees of procedural fairness[31].

3.9. Data subject remedies

Section 33 of the Cyber and Data Protection Act only recognises criminal remedies, except for civil remedies in favour of data subjects. In recognition and codification of the principle that there are no rights without remedies, there is a need for the Act to expressly recognise the right of data subjects to effective judicial remedies against data controllers or processors[32]. In that regard, the Act should express the right of data subjects to receive compensation from a data controller or processor for financial or emotional damage suffered because of infringement of Act[33].

4. Surveillance legislation

As noted above, the main pieces of legislation providing surveillance in Zimbabwe are the Interception of Communications Act and the Postal and TelecommunicationsAct. In that regard, the long title of the Interception of Communications Act states that the purpose of the Act is to "*provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe*". By allowing for interception and monitoring of communications, the Interception of Communications Act and the Postal and Telecommunications Act operate to abridge the constitutional right to privacy, which is defined to include a person's right not to have "*the privacy of their communications infringed*"[34]. While in Section 86 of the Constitution of Zimbabwe, the limitation of the right to privacy is permissible, such limitation must be necessary and proportionate for it to be valid[35]. In that regard, the International Principles on the Application of Human Rights to Communications Surveillance states: *Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.*

29. See Article 45 (2) of the EU GDPR.
30. See Article 61 of the EU GDPR.
31. See the International Principles on the Application of Huma Rights to Communications Surveillance.
32. See Article 19 of the EU GDPR.
33. See Article 82 of the EU GDPR.
34. See section 57 (d) of the Constitution of Zimbabwe, 2013.
35. This can be gleaned from section 86 (2) of the Constitution.

In light of the legitimate need to prevent, detect, and investigate crimes, it cannot be gainsaid that the Interception of Communications Act and the Postal and Telecommunications Act are necessary. The question arises whether the two pieces of legislation pass the proportionality test. Therein lies the rub. The Interception of Communications Act and the Postal and Telecommunications Act are found wanting in various material respects.

4.1. The Interception of Communications Act

4.1.1. Definitions

The Interception of Communications Act uses the word "monitoring" in various instances. For instance, as noted above, the long title of the Act states that its purpose is, among other things, to allow for the monitoring of certain communications. Further, Section 9 (1) (h) (i) of the Act requires postal and telecommunication service providers to have the capacity to allow monitoring by more than one authorised person. However, the interpretation clause of the Act, namely Section 2, does not define the word "monitoring". It follows that there is no indication as to the parameters that authorised persons are required to observe in monitoring communications, thus rendering the process of monitoring communications open-ended and liable to abuse. Accordingly, there is a need to incorporate a definition of the term "monitoring" in the interpretation clause of the Act.

4.1.2. Lack of judicial oversight

In Section 5 of the Interception of Communications Act, as amended, the powers to allow interception of communication are vested in the Minister of Transport and Communications upon advice by the Cyber Security Committee. In terms of Section 4B of the Act, as amended, members of the Cyber Security Committee are appointed by the Minister, and they are drawn from various government agencies such as the National Prosecuting Authority, Central Intelligence Organisation, Zimbabwe Republic Police and POTRAZ. It is submitted that the above-mentioned regime for authorising the interception of communications runs counter to the International Principles on the Application of Human Rights to Communications Surveillance, which provides that: *Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent*. By virtue of being a member of the Executive, the Minister is not a competent judicial authority. By the same token, the members of the Cyber Security Committee are appointees of the very Minister, and they are all drawn from government agencies. Accordingly, neither the Minister nor the Cyber Security Committee meets the independence and impartiality envisaged by international standards. Section 5 of the Act must be amended to vest the powers to issue a warrant of interception of communication in the judiciary.

4.1.3. Bulk Communication Surveillance

Section 9 of the Interception of Communications Act allows for bulk surveillance. Bulk surveillance can be regarded as involving "*the state's monitoring and targeting of a huge section of the population on a continuous basis using digital technology*"[36]. The problem with bulk surveillance is that it is indiscriminate

36. See section 57 (d) of the Constitution of Zimbabwe, 2013.
37. This can be gleaned from section 86 (2) of the Constitution.
38. B. Hungwe & A. Munoriyarwa, An Analysis of the Legislative Protection for Journalists and Lawyers Under Zimbabwe's Interception of Communications Act, 2024 at page 13.

in its approach and fails to distinguish between ordinary communication and protected communication, such as communication involving journalist and legal practitioner privilege. For instance, Section 61 (2) of the Constitution of Zimbabwe defines freedom of media to include protection of the confidentiality of journalists' sources of information. Accordingly, the bulk surveillance permitted by Section 9 of the Act is unconstitutional because it may target communications subject to journalist privilege. There is a need to amend Section 9 of the Act by abolishing bulk surveillance and supplanting it with targeted surveillance.

4.1.4. Handling of intercepted communications

While the Interception of Communications Act allows for the interception of communications, does not lay down the proper procedure to be adopted when authorities examine, copy, share, sort through, use, destroy, and/or store intercepted communication 41. Accordingly, there is a lacuna in the law in that regard that needs to be addressed to put in place safeguards against the misuse and abuse of intercepted communications.

4.1.5. Notification of surveillance

In Section 18 of the Interception of Communications Act, a person notified of or becomes the subject of a warrant authorising interception of their communications may note an appeal to the Administrative Court. However, the Act does not impose a positive obligation on the authorities to notify individuals that they have been the subject of an interception warrant.

According to the International Principles on the Application of Human Rights to Communications Surveillance, *Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision and should have access to the materials presented in support of the application for authorisation.*

In the South African case of *Amabhungane Centre for Investigative Journalism NPC and Another vs Minister of Justice and Correctional Services & 10 Others* Case No. 25978/17, it was held that:
Pre-interception notice is self-evidently problematic. The idea is vulnerable to a cogent argument that to do so defeats the very purpose of the exercise. Thus, the focus of the application is on a post-surveillance-notice".
Accordingly, the Act should be amended to at least explicitly provide for the right of a person whose communication has been intercepted to post-surveillance-notice.

4.1.6. Public oversight

In terms of Section 4A of the Interception of Communications Act as amended, it is the Cyber Security and Monitoring of Interceptions of Communications Centre, which is the sole facility through which authorised interceptions are effected. By the same token, the Cyber Security and Monitoring of Interceptions of Communications Centre oversees the enforcement of the Act to ensure that it is enforced reasonably and with due regard to fundamental human rights and freedoms. In terms of Section 4 (1) of the Act as amended, the Cyber Security and Monitoring of Interceptions of Communications Centre is established as a unit in the Office of the President.

The International Principles on the Application of Human Rights to Communications Surveillance provides that: *States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities, to evaluate whether the State has been transparently and accurately publishing information and scope of communications surveillance techniques and powers, and to publish periodic reports and other information relevant to communications surveillance*". The Cyber Security and Monitoring of Interceptions of Communications Centre is established as a unit in the Office of the President, so it is clear that it does not have the independence and capacity to discharge the mandate contemplated by the International Principles on the Application of Huma Rights to Communications Surveillance. Accordingly, a truly independent and able authority must oversee the conduct of communications surveillance in Zimbabwe. Alternatively, such an oversight mandate may be given to Parliament 42.

4.2. The Postal & Telecommunications Act

In terms of Section 98 of the Postal and Telecommunications Act, a postal or telecommunication licensee or employee of such licensee in charge of a telegraph office is allowed to intercept or detain any telegram which he suspects of having contents that provide evidence of the commission of a criminal offence or of being sent to assist the commission of a crime; or upon request by a commissioned police officer who suspects it of having contents that provide evidence of the commission of a criminal offence or of being sent to assist the commission of a crime. Firstly, Section 98 of the Act does not qualify the suspicion based on which a licensee or employee thereof may act to intercept a telegram. In that regard, the licensee or its employee must be required to act based on reasonable suspicion. This is necessary to introduce a safeguard in the form of an objective test against which the lawfulness of interception of a telegram in terms of the Act may be measured. Secondly, the regime for the interception of telegrams set out in Section 98 of the Act is defective in that it lacks the safeguards mentioned above in relation to the Interception of Communications Act, such as judicial oversight and notification requirements. Accordingly, Section 98 of the Postal and Telecommunications Act needs to be amended in those respects.

5. Recommendations

Considering the preceding, there are various yawning gaps in Zimbabwe's data protection, privacy and surveillance legislation. Accordingly, the following measures are proposed to improve the current state of the relevant legislation.

5.1. Data protection and privacy legislation

5.1.1. Broadening of the scope of sensitive data

The Cyber and Data Protection Act should expressly include biometric data as part and parcel of sensitive data. By the same token, the Act should provide a definition of the term biometric data to avoid doubt.

5.1.2. Limitation of the scope of application of the Cyber & Data Protection Act

The Cyber and Data Protection Act should expressly indicate that it does not apply to the processing of personal data by a natural person during a purely personal or household activity, in accordance with international best standards.

5.1.3. Establishment of a truly independent National Data Protection Authority

The fact that POTRAZ is subject to the executive's control in various material respects detracts from its independence as the National Data Protection Authority envisaged by the best international standards.

Further, the fact that POTRAZ is also the Cyber Security Center and the postal and telecommunications sector regulator means it is stretched thin, thus adversely affecting its ability to effectively fulfil the extensive and onerous functions reposed in the National Data Authority. Accordingly, there is a need to establish a separate and stand-alone entity as the National Data Protection Authority.

5.1.4. Separate and explicit provisions for principles relating to the processing of personal information

Currently, the Cyber and Data Protection Act frames and casts the principles relating to processing personal information as duties of the data con yet principles and duties are different. This gives the impression that the Act conflates the principles relating to data processing and duties of data controllers. Accordingly, there is a need to amend the Act to make separate and explicit provisions for principles relating to the processing of personal information.

5.1.5. Enhancement of the rights of data subjects

To address the currently narrow scope of the bill of data subject rights in the Cyber and Data Protection Act, the Act needs to be amended by enlarging the ambit of data subject rights such as the rights to rectification, erasure, and objection and enshrining new rights such as the rights to restriction of processing and data portability. Data controllers and processors must also be obliged to comply with obligations arising out of data subject rights without undue delay.

5.1.6. Tightening of the obligations of data controllers regarding data security breach The Cyber and Data Protection Act should be amended to oblige the data controllers to notify the data subject of security breaches. This is necessary because the breach is likely to pose a high risk to natural persons' rights and fundamental freedoms.

5.1.7. Imposition of additional obligations on data controllers

The Cyber and Data Protection Act should impose additional duties on data controllers and processors about conducting risk assessments where fundamental rights and freedoms are at stake, preparing standard and adequate privacy policies, and conducting data protection by design and by default.

5.1.8. Tightening of the obligations of data controllers and adoption of international cooperation mechanisms with regards to cross-border transfer

The scope of considerations that a data controller must consider in assessing the adequacy of the level of protection afforded by a third party for purposes of cross-border data transfer in the Cyber and Data Protection Act should be broadened to expressly include the rule of law, respect for human rights and fundamental freedoms, and case law, among other factors. Further, the Act should provide for mutual legal assistance and multilateral and bilateral treaties as a mechanism of international cooperation in enforcing data subject rights in relation to cross-border data transfers.

5.1.9. Provision of civil remedies in favour of data subjects

The Cyber and Data Protection Act should expressly recognise and codify civil remedies that entitle data subjects to receive compensation from a data controller or processor for financial or emotional damage suffered because of infringement of the Act.

5.2. Surveillance Legislation

5.2.1. Definition of key terms

The Interception of Communications Act should include a definition of the term monitoring to guard against abuse of surveillance powers by delineating what the authorities should and should not do while monitoring communications.

5.2.2. Adoption of judicial oversight

The Interception of Communications Act and the Postal and Telecommunications Act should require that decisions related to authorising the interception of communications be made by a competent, impartial, and independent judicial authority.

5.2.3. Adoption of safeguards in respect of the handling of intercepted communications

The Interception of Communications Act and the Postal and Telecommunications Act should stipulate the proper procedure to be adopted when authorities are examining, copying, sharing, sorting through, using, destroying and/or storing intercepted communication.

5.2.4 Imposition of the obligation to notify that surveillance has taken place

The Interception of Communications Act and the Postal and Telecommunications Act should expressly oblige authorities to adequately and properly notify affected persons that they have been subject to the interception of communications.

5.2.5. Abolition of bulk surveillance

The bulk surveillance currently provided for in the Interception of Communications Act should be discarded and supplanted with targeted surveillance.

5.2.6. Adoption of a proper public oversight mechanism

The Cyber Security and Monitoring of Interceptions of Communications Centre provided for in the Interception of Communications Act as amended is not fit for purposes, as it is not independent in terms of best international standards. Accordingly, it should be replaced with an independent and effective public oversight mechanism.

Conclusion

Various yawning gaps impair the effectiveness of data protection, privacy, and surveillance legislation in its present state. Accordingly, this Policy Brief proposes that the above-mentioned recommendations be adopted to align the relevant legislation with international best practices so that it can pass constitutional muster.

REFERENCES

Acts of Parliament
Constitution of Zimbabwe, 2013
Cyber and Data Protection Act [Chapter 12:07]
Census and Statistics Act [Chapter 10:29]
Consumer Protection Act [Chapter 14:14]
Protection Personal Information Act No.4 of 2013
Interception of Communications Act [Chapter 11:20]
Postal and Telecommunications Act [Chapter 12:05]

Regulations
Electoral (Voter Registration) Regulations, 2017 Statutory Instrument 85 of 2017
Postal and Telecommunications (Subscriber Registration) Regulations, 2014 Statutory Instrument 95 of 2014
European Union General Data Protection Regulations

Conventions and Treaties
African Union Convention on Cyber Security and Personal Data Protection
Southern African Development Community Model Law on Data Protection
International Principles on the Application of Huma Rights to Communications Surveillance

Articles & Books
B. Hungwe & A. Munoriyarwa, An Analysis of the Legislative Protection for Journalists and Lawyers Under Zimbabwe's Interception of Communications Act, 2024
Data Protection Laws of the World

Case-law
Amabhungane Centre for Investigative Journalism NPC and Another vs Minister of Justice and Correctional Services & 10 Others Case No. 25978/17

www.misa.org