Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights.

MISA ZIMBABWE

KONRAD ADENAUER STIFTUNG

Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights.

Published By

MISA-Zimbabwe
+263242776165, +263242746838
Website: zimbabwe.misa.org

in partnership with

KONRAD ADENAUER STIFTUNG

Design
OnaDsgn
hello@onadsgn.com
www.onadsgn.com

ISBN: 9781779065353

Contents

Executive summary

This report focuses on enacted and proposed cybersecurity and cybercrime laws in the SADC region and how they have impacted the exercise of rights, more specifically, the right to privacy, freedom of expression and media freedom. It also makes a comparative of these laws with international conventions, standards and norms for instance as found in the provisions of the European Union, African Union, and SADC Model Laws.

This report focuses on countries such as Botswana, Lesotho, South Africa, Namibia, Zimbabwe and Zambia. This study which relies heavily on desktop review and key informant interviews shows that although some countries in the SADC region have enacted cybersecurity and cybercrime laws, others are still in the process of drafting similar laws. On the one hand, countries like Botswana, eSwatini, Tanzania, Malawi and Zambia have already passed cybersecurity and cybercrime laws while countries such as Namibia, South Africa, Lesotho and Zimbabwe have gazetted draft legislation on cybersecurity and cybercrime.

It is also shown in this report that although some of the enacted and proposed cybersecurity and cybercrime laws are modeled along international, regional and sub-regional model laws and other human rights instruments, there are a number of problematic provisions, which infringe on the right to privacy and freedom of expression. Second, while most of the enacted and proposed laws in the SADC region attempt to balance cybersecurity issues with human rights frameworks as espoused in national constitutions, there are still restrictive laws dealing with interception of communication, data protection and electronic transactions.

Third, in countries such as Zambia, Zimbabwe, Namibia and Malawi, there is deep-seated fear that existing and new legislation are already being used for surveillance purposes. For instance, South Africa uses the RICA Act to regulate the interception of communication and Zimbabwe has the Interception of Communications Act while Zambia deploys the Electronic Communications and Transactions Act of 2009. Fourth, there are concerns around broad and vague definitions of criminalised offences and key terms such keystroke, false news, race and xenophobic-related crime, modification, unauthorised access, or asymmetric cryptosystem, cyber terrorism, child pornography and cyber extortion and so forth. Fifth, inadequate oversight or accountability mechanisms over the functions of cyber inspectors, data controllers, internet service providers and ministers pose serious threats to the integrity and effectiveness of the legislation. The minister must ideally report to parliament.

Finally, the study has demonstrated that while some countries have made significant inroads in terms of criminalising cyber-related conduct, providing adequate procedural tools and mapping out international cooperation arrangements, others are still stuck in the 'foggy zone' of procrastination, bickering and slow policy making.

Background

It is now axiomatic that the mass diffusion of the internet and its ancillary digital technologies have created an alternative space for the widespread and 'unrestricted' exercise of rights like freedom of expression, freedom of assembly and access to information especially in contexts where such rights are already curtailed through legal and political repression. It has facilitated the conducting of online transactions, e-learning, remote working, video conferencing and many other political, economic, cultural and social activities. Despite the intractable issue of digital divide and inequalities, the Southern African Development Community (SADC) region has witnessed the growth of internet and social media penetration and use over the last two decades owing to the liberalisation of the telecommunications sector and the advent of advanced wireless technologies such as 3G, 4G and 5G.

The digital space has altered communication patterns with online and social media becoming the preeminent arena for public communication and culture, often giving ordinary citizens a voice that they previously lacked (Mare, 2018). The emergence of e-commerce has also created business opportunities and convenience for citizens, whilst at the same time opening up the space for crime and the possibility of compromising citizens' data security. Ultimately, governments are compelled to enact legislation to govern the online and digital space in order to prevent cyber-related crimes and protect citizens from hackers and fraudsters. In the process, though, the online and digital rights of citizens must be similarly protected as the governments enact these laws. The reality, however, is that many countries have either introduced or are planning to introduce cybersecurity and cybercrime laws that potentially threaten the

rights to free speech, expression association, access to information and privacy amongst others.

In the era of 'surveillance capitalism[1] ' (Zuboff, 2018), the increased use and appropriation of digital technologies has been accompanied by massive information collection and processing, including personal data. Data is being collected, processed, shared and transferred every day, with or without the knowledge of the affected persons, which has serious implications for personal privacy (AFDEC, 2020). Because of this intrusive collection and procession of personal data and information by state and non-state actors, the conceptualization of the right to privacy has become very fluid and complicated. The uptake of facial recognition, video conferencing, contact tracing, artificial intelligence and machine learning technologies has expedited the processing, analysis, collection and storage of data, including personal information (Zuboff, 2018). These technologies have augmented surveillance practices, thereby paving way for the setting up of huge databases with technical capacities to anonymise and de-anonymise data – all on a wide scale. This turn of events has significant implications on the right to privacy. In Southern Africa, Hunter and Murray (2020) have shown that increased interference with the right to privacy mostly exists in environments with limited oversight mechanisms and results in data breaches, misuse of personal data, unlawful and indiscriminate interception of communications and impermissible data retention policies.

Cognisant of the fact that digital rights have become an inseparable part of our everyday lives because of the complex interaction between human beings and digital technologies, scholars have begun to foreground the advent of dark forms of participation such as the spread of misinformation, disinformation, mal-information, cyber-bullying, cyber harassment and revenge porn. This is despite the initial celebratory views of the internet as technologies of freedom and accountability. In recent years, fears about the normalisation of communications surveillance, roll out of invasive monitoring and tracking technologies by governments and corporates, state-ordered Internet shutdowns as well as the passage of draconian pieces of legislation have dominated national, regional and international headlines (Mare, 2020). Instead of promulgating laws that are consonant with the Necessary and Proportionate Principles as articulated by Access Now, Privacy International (PI), Electronic Frontier Foundation (EFF), and Association of Progressive Communications (APC), some SADC countries have brazenly came up with legal frameworks that violate inalienable human rights as enshrined in their national constitutions.

Many governments in the SADC region are taking steps that undermine internet access and affordability, and weaken the potential of digital technologies to catalyse free expression and civic participation or to drive innovation. In a number of SADC countries, there has been an increase in digital rights violations such as arrests and intimidation of online users, internet blockages, and a proliferation of laws and regulations that undermine the potential of technology to drive socio-economic and political development in the region. Several countries have come up with a number of Bills focusing on data protection, electronic transactions, cybercrimes and computer crimes and interception of communications in the last decade. Instead of helping to increase the accessibility and availability of ICTs, some of these pieces of legislation have contributed to

1 It is a "new economic order" and "an expropriation of critical human rights that is best understood as a coup from above".

the restriction of citizens' rights to free speech, privacy and access to information, thereby undermining efforts to bridge the digital divide.

Internet shutdowns in particular during elections and during public protests and demonstrations are becoming commonplace (Mare, 2020). State surveillance in cyberspace as well as private spaces is on the increase, limiting civic space for engagement and critical opinion, and further curtailing an enabling environment for such engagement (Hunter and Mare, 2020). In addition, insult laws such as those meant to protect Heads of State and Government and other senior government officials from scrutiny and criticism have been invoked to limit public debate on social media regarding governance, democracy and human rights. Laws to protect the integrity of e-commerce have been used to prevent non-governmental organisations and human rights defenders from opening and operating bank accounts and from transacting, thereby curtailing their work. All these issues have brought to the fore the debate about the need for States to balance the regulation of the digital/online space or prevent online crime and the promotion and protection of citizens' digital/online rights.

However, the spread of ICTs and Internet penetration has also raised concerns about cyber security at regional and sub-regional governance forums (Orji, 2015, 105). This has led African intergovernmental organisations to develop legal frameworks for cyber security. At a sub-regional level, the Economic Community of West African States (ECOWAS) has adopted a Directive on Cybercrime, while the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) have adopted model laws. In Southern Africa, there are three model laws worth mentioning here. These are

1) The SADC Model Law on Computer Crimes and Cybercrimes;

2) The SADC Model Law on Data Security; and

3) The SADC Model Law on Electronic Transactions and Electronic Commerce.

At the regional level, the African Union (AU) has adopted a Convention on Cyber Security and Personal Data Protection. Individual countries like Zambia, Botswana, Tanzania, and Malawi have enacted cybersecurity laws as part of their internet governance frameworks while in countries like Zimbabwe, South Africa and Namibia plans are afoot to pass the similar legislation.

Unfortunately the developed and or proposed legal frameworks have been narrowed down to entirely prioritising the protection of 'national interests' and the prevention of 'social media abuse' at the expense of the digital security and protection privacy of general and day-to-day internet users in the SADC region. These instruments have therefore also been characterised as vehicles for legitimising surveillance and criminalising free expression in the SADC region. The situation has been made worse by the fact that ever since the fast spreading of the novel coronavirus (also known as COVID-19), almost every facet of human life has been forced to migrate online in order to circumvent lockdown, social distancing and self-isolation protocols. In this 'new normal', the internet and digital media technologies have become indispensable part of learning, news consumption, e-commerce, accessing government documents and contact tracing. This digital turn in everyday life has been accompanied by concomitant digitisation of criminal conduct. In view of these concerns, MISA-Zimbabwe commissioned this particular study, which specifically focuses on the analysis of the enacted and proposed cyber laws in the SADC region and how they have impacted the exercise of rights more specifically, the right to privacy, freedom of expression and media freedom.

The right to privacy is guaranteed in international and regional human rights instruments. It is enshrined in over 130 national constitutions across the world. It is enshrined in article 12 of the UDHR, article 17 of the ICCPR, article 16 of the Convention of the Rights of the Child (CRC), and article 10 of the African Charter on the Rights and Welfare of the Child (AFDEC, 2020). The African Charter does not have a provision on the right to privacy, but this right has been acknowledged under the Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) (the Declaration).

Key international and regional standards that protect the right to privacy and freedom of expression:

Universal Declaration on Human Rights (UDHR)

International Covenant on Civil and Political Rights (ICCPR)

General Comment No. 34 on Article 19 of the ICCPR (General Comment No. 34)

African Charter on Human and Peoples' Rights (African Charter)

Declaration of Principles on Freedom of Expression in Africa (African Declaration on Freedom of Expression)

African Charter on Democracy, Elections and Governance (ACDEG)

Overall Objectives

The overall objective of this report is to critically analyse the impact of cybersecurity laws on exercise of rights in selected SADC countries. It falls within the broader ambit of the media freedoms and digital rights. As such, it aims to contribute towards the recognition, awareness, and enforcement of human rights in the Southern African Development Community (SADC) region.

This report looks at the following thematic issues:

An overview of how the internet space has impacted the exercise of rights;

Highlight regional and international legal frameworks on cybercrimes and cybersecurity and the key principles highlighted therein for the protection and promotion of rights;

Analysis of cybersecurity laws in the Southern African region and how they impact the exercise of rights including countries like Zimbabwe, Botswana, Lesotho, South Africa, Namibia and Zambia;

Assess the circumstances in which these laws have been relied on for surveillance purposes or to curtail free expression; and

Provide strategies that can be relied on to ensure that these laws promote instead of curtailing exercise of rights.

Conceptual Framework

This report is anchored on the human rights-based approach. It foregrounds the point that the 13 necessary and proportionate principles are important in the drafting of progressive legislation on cybercrimes and cybersecurity issues. A human rights-based approach (HRBA) is grounded on the principles drawn from international and regional treaties, and places human rights as the centre of all policy making and drafting of legislation. Some of the core principles of the human rights-based approach include: participation, accountability and transparency, non-discrimination and equality, empowerment of rights holders and legality. Thus, the incorporation of the human rights-based approach ensures that policymakers are able to meet their human rights obligations, and achieve better outcomes that benefit rights-holders. This can be done through integrating international human rights system norms, principles (necessary and proportionate principles) and standards (model laws) and goals.

In a nutshell, an HRBA puts emphasis on clearly defining the rights of right holders and corresponding obligations of duty-bearers; examining reasons for failure to realise some human rights objectives; and assessing the capacity of rights holders to claim their rights from duty bearers and develop strategies to enhance those capacities (AFDEC, 2020). It also entails using human rights standards and principles in monitoring and evaluation of outcomes and processes. Below are some of the key principles of the HRBA:

Table 1: Key principles of the HRBA

- Interdependence and interrelatedness: Human rights are by their nature symbiotic and interrelated. Each right has a contributory effect on other rights, which could be positive or negative. For example, the realization of the right to privacy can contribute to the enjoyment of freedoms of association and assembly. Similarly, the fulfilment of the right of freedom of expression could be dependent of rights such as the right of access to information and right to privacy.
- Equality and non-discrimination: This principle is embedded in international norms and standards that all human beings are equal and dignity is inherent in every person. Discrimination should be prohibited, whether on the grounds of political, language, sexual orientation, religion, colour, ethnicity, gender, race, age or other opinion, national, social or geographical origin, disability, property, birth or other status, as acknowledged by human rights norms standards.
- Participation and inclusion: The principle of participation underpins the essence of a HRBA. It is based on the notion that all people have the right to participate in the decision- making processes that affect their wellbeing and lives. The participation is also centred on the principle of non-discrimination and equality. For participation to be successful and effective, rights-holders require adequate and credible information.
- Accountability and rule of law: The state has the obligation to protect human rights as mandated under international law and standards that states sign up to. They are answerable and must comply with human rights obligations. Duty-bearers are also answerable in the observance of human rights. Failure to comply should attract sanction and remedies for rights holders. The public and private sectors, such as the media, community, and civil society, are instrumental in holding the government accountable for not upholding their obligations.

Source: AFDEC Data Protection Toolkit (2020)

Closely connected with the human rights-based approach is the Necessary and Proportionate Principles as articulated by Access Now, Electronic Frontier Foundation, Privacy International and Association of Progressive Communications. The principles foreground international human rights law especially as it relates to issues like the protection of privacy, freedom of expression, and the rule of law. The principles outline how communications surveillance can be conducted consistent with human rights and can serve as a model for reform worldwide.

Table 2: Summary of the 13 Necessary and Proportionate Principles

Legality: Limits on the right to privacy must be set out clearly and precisely in laws, and should be regularly reviewed to make sure privacy protections keep up with rapid technological changes.
Legitimate Aim: Communications surveillance should only be permitted in pursuit of the most important state objectives.
Necessity: The State has the obligation to prove that its communications surveillance activities are necessary to achieving a legitimate objective.
Adequacy: A communications surveillance mechanism must be effective in achieving its legitimate objective.
Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Proportionate communications surveillance will typically require prior authorization from a competent judicial authority.
Competent Judicial Authority: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.
Due Process: Due process requires that any interference with human rights is governed by lawful procedures which are publicly available and applied consistently in a fair and public hearing.
User Notification: Individuals should be notified of a decision authorizing surveillance of their communications. Except when a competent judicial authority finds that notice will harm an investigation, individuals should be provided an opportunity to challenge such surveillance before it occurs.
Transparency: The government has an obligation to make enough information publicly available so that the general public can understand the scope and nature of its surveillance activities. The government should not generally prevent service providers from publishing details on the scope and nature of their own surveillance-related dealings with State.
Public Oversight: 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.
Integrity of Communications and Systems: Service providers or hardware or software vendors should not be compelled to build surveillance capabilities or backdoors into their systems or to collect or retain particular information purely for State surveillance purposes.
Safeguards for International Cooperation: On occasion, states may seek assistance from foreign service providers to conduct surveillance. This must be governed by clear and public agreements that ensure the most privacy-protective standard applicable is relied upon in each instance.

Safeguards Against Illegitimate Access: There should be civil and criminal penalties imposed on any party responsible for illegal electronic surveillance and those affected by surveillance must have access to legal mechanisms necessary for effective redress. Strong protection should also be afforded to whistleblowers who expose surveillance activities that threaten human rights.

Source: Electronic Frontier Foundation

International standards and best practices stress that any limitation to fundamental rights should pass the three-pronged test on legality, necessity and proportionality. For instance, principle 41 of the Declaration on Principles of Freedom of Expression and Access to Information in Africa of the African Commission on Human and Peoples' Rights, outlines the following:

1. States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications.
2. States shall only engage in targeted communication surveillance that is authorised by law, that conforms to international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.
3. States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including:
4. the prior authorization of an independent and impartial judicial authority;
5. due process safeguards;
6. specific limitation on the time, manner, place and scope of the surveillance;
7. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
8. proactive transparency on the nature and scope of its use; and
9. effective monitoring and regular review by an independent oversight mechanism.

Although some Southern African countries are not bound by the International Principles of Human Rights in relation to Electronic Communications, which was drafted by the United Nations, the instrument clearly spells out how human rights should be protected in electronic communications. It also states that limitations of human rights should only occur if necessary and should be proportional to the aim, which the limitation strives to achieve.

A brief overview of the literature review

The mass diffusion of digital media technologies have been accompanied by several social vices, which have prompted several countries in Southern Africa to enact domestic cybercrime legislations (Orji, 2015). In view of the necessity to come with legislation that protect citizens from cyber fraudsters, criminals, hackers and other malicious actors who use digital media technologies to commit heinous crimes, national governments have been busy since the turn of the century coming with laws. Most of the laws that have been enacted or currently being drafted have focused on addressing cybercrimes, cyber-security, and electronic transactions and data protection. Cybercrimes are refers to crimes, which are committed through the internet using a computer. This includes a wide range of offences against computer data and systems (such as 'hacking'), computer-related forgery and fraud (such as 'phishing'), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).

Cyber-security denotes the protection of computer networks, programs and other internet connected systems from cyber-attacks. In the era of e-learning, e-commerce, mobile payment platforms, e-voting and e-government, cyber-attacks could do irreparable and irreversible damage to businesses and persons. This includes the misuse of personal information such as email addresses and credit card information, or huge financial losses to multinational organisations. Cyber-security intends to reduce cyber-security risks, to minimise successful cyber-security attacks, and to build trust in and security of the internet. It encapsulates the application of information security standards, the definition of appropriate cyber-security organisations and the education of internet users. In light

of these serious criminal offenses, it has been acknowledged that there is need to find a delicate balance between criminalisation of certain uses of technologies whilst at the same time upholding constitutionally-guaranteed rights like freedom of expression, assembly and press freedom.

Most cyber-crimes and computer laws have foregrounded provisions such as confidentiality, integrity and availability of computers systems, search, hacking and mutual international cooperation. Because of the transnational nature of cybercrimes, the perpetrator may be located in one country whilst the victimized person, computer system or data is located in another country (Orji, 2015). This follows that the perpetrators may also use computer systems or networks in other countries as an attack base (what is called "remote attacks") or as a route to reach their victims (Orji, 2015). This suggests that the detection of cybercrimes, identification of perpetrators, the gathering of the necessary evidence and the prosecution of suspected cyber criminals often require the cooperation of authorities from multiple jurisdictions. As Brenner and Shwerha (2008) observe, harmonisation of cybercrime legislations help to eliminate "cybercrime safe havens". In short, international cooperation and harmonisation are indispensable components in any strategy against cyber-crime. Besides incorporating the mutual international cooperation provisions, there is also a call for these legislations to address country-specific challenges and needs. Over and above these concerns, there is need to ensure the enacted and proposed laws are comply with the necessary and proportionate principles.

Although the African continent is late to jump onto the bandwagon of cybercrimes and cybersecurity laws, they have begun to take keen interest on the matter. Some of the reasons for the late enactment of cybercrimes legislations could be attributable the low penetration of ICTs in Africa prior to the widespread proliferation of wireless technologies in the last decade. However, the situation has changed dramatically in the last few years with the adoption of 3G, 4G and 5G technologies, which has spurred massive growth in mobile internet penetration and smartphone usage. This growth in internet penetration has been accompanied by an upsurge in cyber-related crimes, digital media activism, citizen journalism, spreading of false news, hacking scandals and whistleblowing. As Mare (2018) observes, the mass permeation of digital technologies in sub-Saharan Africa has been accompanied by dark forms of participation related to cyber-bullying, mis-and disinformation, revenge and child pornography, networked xenophobia, brigading (retrogressive role of cyber-troops and troll armies), and production of race and ethnic-related hate speech. These insidious forms of participation have alerted national governments on the desirability of coming up with cybercrimes and cybersecurity legislations to curb the abuse of digital media technologies.

Some countries have used the unprecedented circulation of false and misleading information via social media platforms as a pretext to justify the promulgation of cyber-crimes laws. Critical infrastructure like telecommunications networks, power networks, (nuclear) power plants, and industrial complexes are potential targets of cyber-attacks, which could have devastating consequences if not adequately countered. In order to fend off these threats, Southern Africa countries are setting up Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

It is generally acknowledged across the board that cyber-crime and cyber-security have

become issues of national and regional importance. It is within this context that the promulgation of cyber laws in the region have been identifies as critical in order to underpin the realisation of full potentials in regional e-commerce, electronic financial transactions and business processes outsourcing. Extant research suggests that no single existing agency can claim a comprehensive understanding and a sufficiently wide authority to manage all facets of cyber-security and cyber-crime. Therefore, effective coordination across government and its agencies, as well as co-operation at an international level are of paramount importance.

METHODOLOGY

The research design guiding this evaluation was framed within a participatory qualitative research methodology. The qualitative methodology will be applied in order to feed the quantitative methodology. Qualitative research integrates the methods and techniques of observing, documenting, analysing, and interpreting characteristics, patterns, attributes, and meanings of human phenomena under study (Gillis & Jackson, 2002; Leininger, 1985). Lincoln (1992) argues that qualitative methods are naturalistic, participatory modes of inquiry that disclose the lived experiences of individuals. Consequently, "there is no single, objective reality, there are multiple realities based on subjective experience and circumstance" (Wuest, 1995: 30).

Data Collection Instruments

Document analysis

Document analysis is a form of qualitative research that was be employed in this study. Through this method, the researcher was able to analyse legislation and policy documents, including international regional, sub-regional and national legislation model laws and legislation on cybersecurity and cyber crime. This information was analysed in order to make sense of the policy and legal implications

of the enacted and proposed legislation on the right to privacy and freedom of expression in selected SADC countries.

Desk Review

Building on document analysis, the report relied heavily on desk review of model laws, best practices and national legislation on cybersecurity and cybercrime. This entailed the systematic analysis of information that already exists, in one form or another. Desk review involves the summary, collation or synthesis of existing research rather than primary research where data is collected from subjects. Sources of desk review included: journal articles, newspapers, books, model laws, periodic reports and so forth culled from organisations such as Misa-Zimbabwe, FES Media, International Media Support, IFEX, CIPESA, Paradigm Initiative, Right to Know Campaign, Paradigm Initiative and Southern Africa Litigation Centre. Secondary data can be a valuable source of information for gaining knowledge and insight into a broad range of issues and phenomena. This secondary provided a cost-effective way of understanding the state of regional, national and international legal frameworks on cybercrimes and cybersecurity and the key principles highlighted therein for the protection and promotion of rights.

Key Informant interviews

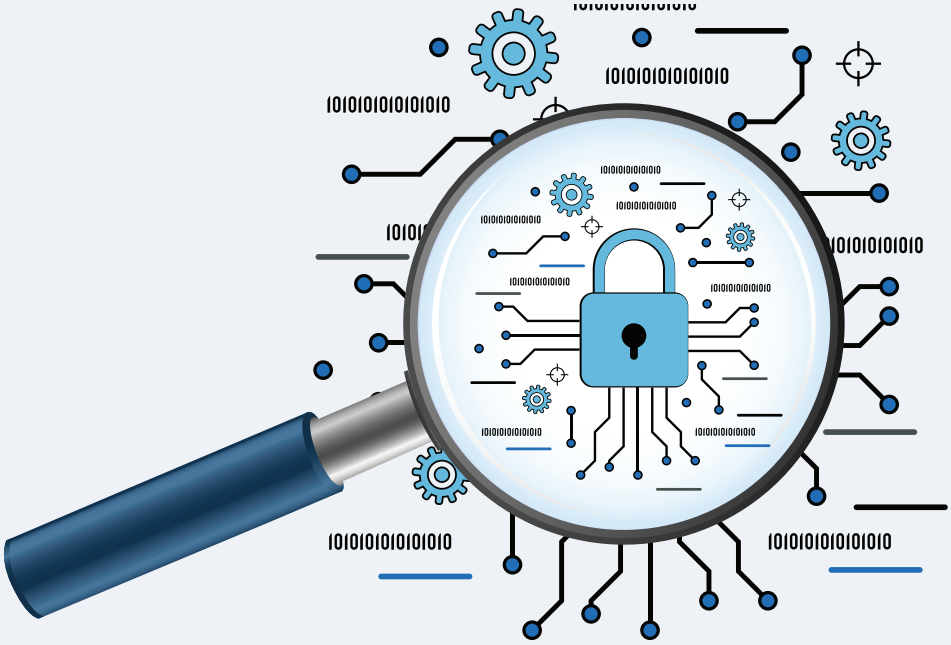
Key informant interviews are qualitative in-depth interviews with people who know what is going on with regards to the circumstances in which cybersecurity and cybercrime laws have been relied on for surveillance purposes or to curtail free expression and strategies that can be relied on to ensure that these laws promote instead of curtailing exercise of rights in the SADC region. The purpose of key informant interviews was to collect information from a wide range of people—including freedom of expression activists, legal practitioners, journalists and human rights defenders. Because of the COVID-19 lockdown protocols and movement restrictions, the researcher used Zoom and WhatsApp to interview 12 respondents from Zimbabwe, Botswana, South Africa, Namibia and Zambia. These people, with their particular knowledge and understanding, were able to provide insight on the circumstances in which these laws have been relied on for surveillance purposes or to curtail free expression and provide strategies that can be relied on to ensure that these laws promote instead of curtailing exercise of rights. Ethical considerations such as informed consent, confidentiality and privacy were strictly observed.

Data Analysis and Interpretation

Qualitative data was analysed using a combination of thematic and narrative analysis. This allowed the researcher to focus on themes, statements or meanings that emerged from desktop research and key informant interviews.

Key findings

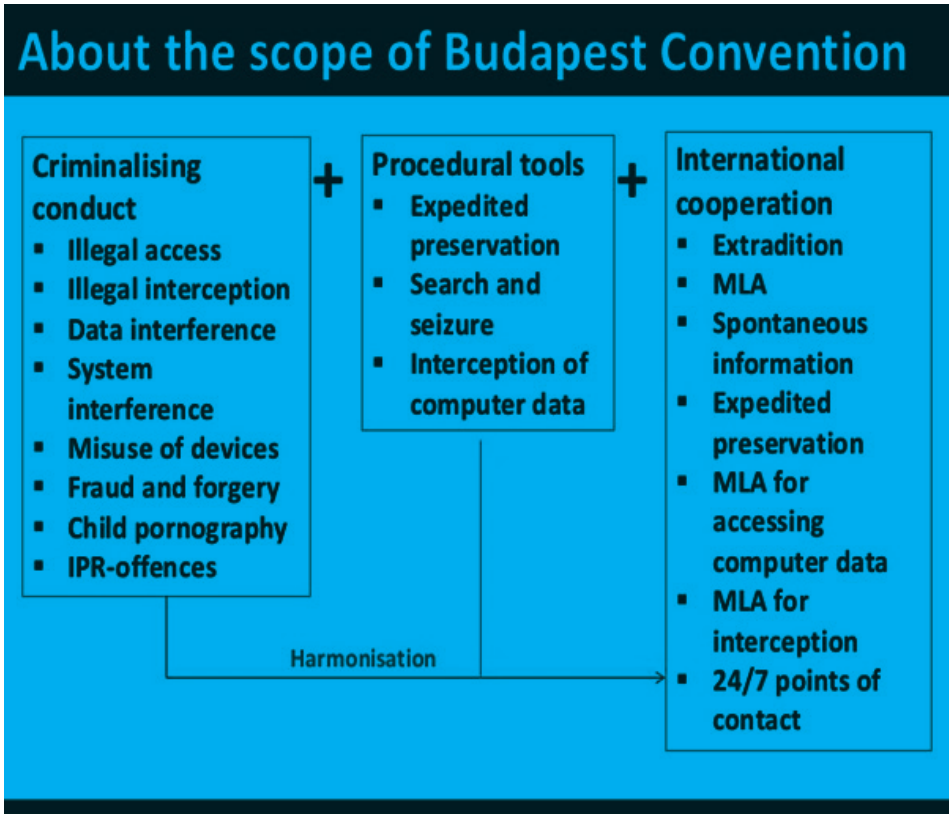
International Legal Frameworks on Cybercrimes and Cybersecurity and the Key Principles



The Budapest Convention on Cybercrime

The Convention on Cybercrime (also known as the Budapest Convention) is the first international convention set out to pursue a common criminal policy against cybercrime (Keller, 2011). It promotes the harmonisation of national laws, capacity building, and the fostering of international cooperation. The Convention was developed by the Council of Europe and became operational on 1 July 2004. The Convention facilitates the detection, investigation and prosecution of crimes committed via the internet and other computer systems including aiding or abetting the commission of an offence.
It criminalises conduct such as illegal access and data interference. It provides the procedural tools for states to follow, this includes search and seizure of computers and other devices used in the criminal activity. It places upon States an obligation for mutual cooperation in assisting with the investigations. The Budapest Convention is further supplemented by an Additional Protocol adopted in 2003, which makes using computer networks to publish xenophobic and racist propaganda, a punishable offence.

Figure 1: The Scope of the Convention



Source: Seger (2016)

The Convention emphasises the importance of maintaining a proper balance between the interest of law enforcement and respect for fundamental human rights, specifically the right to hold opinions without interference, freedom of expression and the rights concerning the respect for privacy. Some of key aims of the Convention is to pursue a common criminal policy aimed at the protection of society against cybercrime; build the capacity of countries to combat cybercrime; and function as a mutual information sharing channel in order to facilitate better law enforcement. It calls upon member states to adopt legislative and other measures to establish the offences listed in Convention as criminal offences under its domestic law. With regards to international cooperation, the Convention calls upon member states to provide mutual[2] assistance to states investigating crimes under the Convention; allow search and seizure of stored computer data for investigations; extradite those charged with cybercrimes or prosecute them domestically; real-time collection of internet traffic data including IP addresses and email header information; and preserve computer data for up to 90 days. The

2Mutual Legal Assistance (MLA) – is an agreement between two or more States to gather and exchange information in an effort to enforce criminal law.

Convention sets a normative standard within the international legal framework, acknowledging the need to pursue a common criminal policy and procedural law in relation to cybercrimes. It promotes cooperation between State parties and the private sector.

The Convention categorises cybercrimes into four broad types: the first involves "offences against the confidentiality, integrity and availability of computer data and systems"; the second are "computer-related offences"; the third are "content-related offences"; and the fourth are "offences related to infringements of copyright and related rights." The first type of cybercrimes penalises activities that target and compromise the confidentiality, integrity and availability of computer data and systems. It clearly spells out five offenses: illegal access to computer systems (article 2); illegal interception of data (article 3); data interference (article 4); system interference (article 5); and misuse of devices (article 6).

In spite of some of the progressive provisions, the Convention has received a fair share of criticism. For instance, some countries have raised sovereignty concerns over the Convention's article 32 that raises the possibility for trans-border access to data without the authorization of public authorities in the country where the data is being stored. The Convention has been criticized for being outdated, having been overtaken by technological and cybercrime developments that have occurred since its adoption in 2001. It does not cover a wide range of cybercrimes including identity theft, sexual grooming of children, and unsolicited emails and spam. It has limited enforcement because over two-thirds of States have not ratified the treaty. Overall, it is important to note that despite the aforementioned criticisms, the Convention remains the only international agreement that addresses cybercrime and is aimed at harmonising national laws and establishing international cooperation against cybercrime in the digital age.

The AU Convention on Cyber Security and Personal Data Protection

In July 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection. The Convention aims to harmonise the laws of African States on electronic commerce, data protection, cyber security promotion and cybercrime control. The objective of this Convention was to propose the adoption at the level of the African Union, a Convention establishing a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.

The AU Convention is broader than the Budapest Convention in that it covers:

Chapter I – Electronic transactions

Chapter II – Personal data protection

Chapter III – Cyber security and cybercrime.

The AU Convention unites different aspects related to information technology law, also including certain non-digital and non-criminal justice issues. It recognises that cybercrime "constitutes a real threat to the security of computer networks and the development of the Information Society in Africa". In this regard, it imposes obligations on Member States to establish national legal, policy and institutional governance mechanisms on cyber security. According to Article 28 of the Convention, there is need for member states to facilitate international cooperation on cyber security. It also requires AU Member States to make use of existing channels of international cooperation (including intergovernmental or regional, or private and public partnerships arrangements) for the purpose of promoting cyber security and tackling cyber threats.

The Convention emphasises the need for States to adopt the principle of double criminality (dual criminality) when rendering cross-border assistance on cyber security issues without creating any mechanisms for Member States to fulfill extradition and mutual assistance requests in the absence of an extradition treaty or mutual assistance arrangement on the basis of dual criminality. Article 28: 1 of the Convention provides that: "State parties shall ensure that the legislative measures and/or regulations adopted to fight against cybercrime will strengthen the possibility of regional harmonisation of these measures and respect the principle of double criminal liability".

Unlike the Budapest Convention, the Malabo Convention explicitly defines some of key terms such as child pornography, computer system, cryptology, cryptology tools, cryptology service provider, data controller, data subject, double criminality, electronic communication, electronic mail, electronic signature, encryption, personal data, racism and xenophobia in information and telecommunication, sensitive data, and third party. For the purposes of this report, Article 8 of the Convention which deals with personal data explicitly points out that:

Each party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data

It adds that:

The mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established.

Article 11 of the Convention calls upon Member States to establish independent National Protection Authorities. It outlines the duties and powers of National Protection Authorities. In Article 13, it outlines the principles governing the processing of personal data. These include: consent and legitimacy of personal data processing, lawfulness and fairness in personal data processing, purpose, relevance and storage of processed personal data, accuracy of personal data, transparency of personal data processing, and confidentiality and security of personal data processing. It discusses the rights of the data subject such as right to information, right to access, right to object, and right of rectification or erasure. It outlines that the personal data controller has obligations to ensure that processed data is confidential, secure, sustainable, and that storage is not too long.

Article 25 of the Convention empowers member states "to adopt legislative and/or regulatory measures as it deems necessary to confer specific responsibilities on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory and legal capacity to act in all aspects of cyber security application". However there is a caveat to this provision as the Convention clearly explains that, "each State Party shall ensure that measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."

The AU Convention provide for a sub-set of procedural powers that are also contained in the Budapest Convention and that are useful for investigating and prosecuting cybercrime

and securing electronic evidence in domestic investigations. The AU Convention does not contain specific provisions and does not constitute a legal basis for international cooperation on cybercrime and electronic evidence.

Like any other convention, it has been criticized for granting too much power to the government, particularly in accessing private information, processing of personal data and sensitive data without consent of the owner for the purpose of state security and public interest could be misused. It gives broad and unchecked powers to "investigating judges". Such powers include the power to issue search and seizure warrants for any electronic records. Another weakness of the Malabo Convention is that it is not a treaty hence has no binding authority on members of the African Union.

The SADC model law

As intimated earlier, the SADC model laws include: Data Protection, Electronic Transactions and Electronic Commerce, and Computer Crime and Cybercrime. The SADC Model Law on Cybercrime, which was launched in 2012, seeks to guide and facilitate the harmonisation of domestic laws on cybercrime. It was adopted in 2013 as part of the Harmonisation of the ICT Policies in Sub-Saharan Africa project (HIPSSA) project. Ever since, the promulgation of the model law some member states have enacted or are in the process of enacting, cybercrime-related legislation.

The aim of the Model Law on Computer Crime and Cybercrime is to offer guidance on how cybercrime and cybersecurity can be regulated by the SADC member states. The SADC Model Law, which was produced 8 years ago, identifies offences that can be incorporated into national laws for the combating of cybercrime. These offences include illegal access, interception, data interference, espionage, forgery, fraud, pornography, xenophobic material and disclosure of details of an investigation.

On the issue of interception of data and preservation of metadata, the model law stipulates the following:

If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data

that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an application a [judge] [magistrate] authorises an extension for a further specified period of time.

Despite its noble intentions, legal analysis has shown that certain provisions in the SADC Model Law on Computer Crime and Cybercrime negatively affect the fundamental right to privacy (Hove, 2017). Because of the anti-privacy provisions inserted in some SADC member States' national Computer and Cybercrime laws, there has been a regional attack on the right to privacy (Hove, 2017). It is important to highlight that the SADC Model Law on Cybercrime has a number of provisions that actively infringe on the fundamental right to privacy. These include section 25 which address issues related to search and seizure of electronic equipment suspected to have been used to commit an offence or suspected to contain information proving the commission of an offence. The main problem with this section is that warrants issued for the search of computers are open to a wide application that one warrant can be used to search all the devices connected to a network of devices (Hove, 2017).

Another problematic part of the model law is section 30, which deals with the collection of network traffic data. Equally concerning is section 31 of the model law, which speaks to the issue of interception of (device) content data. It can easily be used to justify intrusive communications surveillance. Section 32 of the Model Law condones the use of keystroke logging software and hardware. In Section 32, keystroke loggers[3] are erroneously categorized as "forensic tools" when in actual fact keystroke loggers are privacy breaching or hacking tools. This therefore makes it possible to gain illegal access to passwords and usernames used on the electronic device which has a key stroke logger installed on it. There is need for better procedural safeguards, and more judicial oversight when using such potentially harmful technology against citizens.

SADC country-specific laws

In Southern Africa, countries such as Botswana (Cybercrime and Computer Related Crimes Act), Tanzania (Cybercrimes Act), Mozambique (Electronic Transactions Act) and Malawi (Electronic Transactions and Cyber Security Act) have come up with legislation to address the thorny issues of cybersecurity and cybercrimes. Other SADC member States such as Mauritius, Botswana, and Zambia already had national cybercrime laws in place before the adoption of the SADC Model Law. These cybercrime laws which were passed on or before 2013 are generally less likely to infringe on the right to privacy when compared to national cybercrime laws passed after adoption of the SADC Model Law.

As a result, Botswana, and Zambia modeled their respective cybercrime laws after international cybercrime instruments and laws, as opposed to the contentious SADC Model Law. Countries, which passed their national laws on cybercrimes

3A keystroke logger can either be hardware or software installed on a computer or other electronic device for the purpose of recording information as it is entered into that electronic device.

after 2013 have been criticised for copying and pasting vague and broad definitions on cybercrimes from the model law. There is also concern that the "cut and paste approach" adopted by most SADC countries have reproduced problematic provisions that are specified in the model law.

Botswana

In Botswana, the Cyber Crime and Computer Related Crimes Act was passed in 2018. In section 4 of the Act, it criminalises "unauthorised access [4]to a computer or computer system". The first type of conduct covers a typical illegal access to a computer system, whilst the second part expands the ambit of the criminalisation to include causing a computer system to perform any function after gaining unauthorised access. The term "access" is defined to mean, "instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer or computer system" (section 2). That definition is wide, and covers the initial entering of a computer system as well as subsequent acts, for instance, storing and retrieving data, or using the resources of a computer.

It follows that a person who has the authorisation to enter a computer system, but has no authorization to store or retrieve data from the computer system, would commit the offence if he or she stores data in, or retrieves data from, the computer system. It also means that merely instructing or communicating with a computer system, without actual entry into the system, amounts to an offence under the section. That definition is wide, and covers basic unauthorised entry into a computer system (as envisaged by the Budapest Convention), as well as other activities such as instructing a computer system, communicating with a computer system, storing and retrieving data from a computer system, as well as using the resources of the computer system.

According to section 9 of the Act, it is an offence for any person to intercept (a) any non-public transmission to, from or within a computer or computer system; or (b) electromagnetic emissions that are carrying data, from a computer or computer system. The person must act "intentionally", "by technical means" and "without lawful excuse or justification". Although this definition incorporates all the key definitional elements of the offence of data interception as prescribed by the Budapest Convention, it has not be localized to speak to the context of Botswana. Overall, it chimes with the requirements under the Budapest Convention, which are that there must be an interception, through technical means, of a non-public transmission of computer data to, from or within a computer or computer system. Under section 7, the Act provides for data interference, which seeks to punish any person who either destroys, deletes, suppresses, alters or modifies data or renders data meaningless, useless or ineffective. In order to be charged under this offense, the person must act "intentionally" and "without lawful excuse or justification." This is in line with the Budapest Convention. Section 8 of the Act punishes any person who either hinders or interferes with the functioning of a computer or computer system or hinders or interferes with

4A person commits the offence if he or she either accesses the whole or any part of a computer or computer system, knowing that such access is unauthorised or causes a computer or computer system to perform any function as a result of unauthorised access to such system.

a person who is lawfully using or operating a computer or computer system. Section 8(2) defines the term "hinder" as including cutting electricity supply to a computer or computer system; causing electromagnetic interference to a computer or computer system; corrupting a computer or computer system by any means; inputting, deleting, altering or modifying data; and impairing the connectivity, infrastructure or support of a computer or computer system. By including an offline conduct of cutting electricity supply to a computer or computer system, it can be argued that the parliament in Botswana intended to cast the ambit of criminalisation wide, by capturing all acts of interference with computers and computer systems.

Section 10 of the Act criminalises a number of activities. Thus section 10(1) punishes any "person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act" (article 10(1)). The wording of the section gives one the impression that the devise need not be designed or adapted primarily for the purposes of committing cybercrimes, and that dual-use devices are covered.

However, the requirement that the person must act "without lawful excuse or justification" saves the day, as dealing in such dual-use devices for non-criminal and legitimate purposes would not be "without lawful excuse or justification". Section 10(2) targets any "person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1)". The targeted conduct under this subsection consists of either receiving or possession of any device designed or adapted for the purpose of committing an offence. Such receiving or possessing must be without lawful excuse or justification, which means that receiving or possessing such a device for some lawful use is not covered. Section 10(3) stipulates that, any "person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act", the subsection targets those who are found in possession of computer data or programme, with the specific intention of using them to commit or facilitate the commission of an offence under that statute. That actual intention must be objectively proved, and not merely inferred from the act of possession.

The Act also criminalises offences such as cyber fraud, cyber extortion, cyber harassment, cyber stalking, offensive electronic communication, production and circulation of pornographic and obscene materials, revenge pornography, racist or xenophobic material, racist or xenophobic motivated insult and unlawful disclosure by service provider. Some of these offences attract a jail term of up to 2 years or P 40 000 fine, or to both. However, anyone who commits child pornography is liable to a fine not exceeding P100 000, or to imprisonment for a term not exceeding five years, or to both.

It also has a punitive sentence for unlawful disclosure by service providers. For instance, section 23 says that, "A service provider who, without lawful authority, discloses — (a) that an order under this Act has been made; (b) any act done under an order; or (c) any data collected or recorded under an order, commits an offence and is liable to a minimum fine of P1 000 000 but not exceeding P5 000 000". With regards to procedural powers, section 24 of the Act explains that, "A police officer or any person authorised by

the Commissioner [5] or by the Director-General[6] , in writing, may, upon confirmation by the court and as soon as reasonably practicable to do so, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification".

As far as search, access and seizure are concerned, the Act outlines that, "Where a police officer, or any person authorised by the Commissioner or by the Director-General, in writing, has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply to a judicial officer for the issue of an order to enter any premises to access, search and seize such data or information". It also provides for real-time collection of content and traffic data. However, this may be done by when a police officer has been granted permission by a judicial officer to compel a service provider, "within its technical capabilities, to— (i) effect such collection and recording referred to in paragraph (a), or (ii) assist the person making the application to effect such collection and recording".

Lesotho

Like Zimbabwe, Lesotho has also gazetted the Computer Crime and Cyber Bill in 2020. The objectives of the Bill is "to criminalise offences against computers and network related crime; to provide for investigation and collection of evidence for computer and network related crime; to provide for the admission of electronic evidence for such offences, and to provide for matters connected with or incidental to the foregoing". In general, the proposed law provides a legal framework for the criminalisation of computer and network related offences.

Building on the SADC and Commonwealth Model Laws on cybercrime, the draft Bill defines key terms such as computer system, access provider, hinder, critical infrastructure, interception, internet service provider, racist and xenophobic material, traffic data, seize and so forth. The Bill defines "computer system" or "information system" as "a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function". Part two of the Bill deals with criminal law provisions. Most of the offences outlined in this section puts intention at the centre of the commission of the offence. For example, it stipulates that, any "person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification…" It criminalises offences such as illegally accessing and remaining logged into a computer system without lawful excuse or justification, obstructing, interrupting or interfering with the lawful use of computer data and disclosing details of a cybercrime investigation, data espionage, harassment, and interception and system interference. However, some of these offences are already addressed in the Penal Code and the Communications Act (section 44).

Like the AU, European Union and SADC Model Laws, the draft Bill provides procedures to determine jurisdiction over criminal offences. In sections 25, the Bill enumerates that "the courts in the Kingdom of Lesotho shall have jurisdiction to try any offence under this Act or any regulations made under it where an act or

5Commissioner of Police appointed by the President in terms of section 112 of the Constitution
6Director-General of the Directorate on Corruption and Economic Crime appointed by the President in terms of section 4 of the Corruption and Economic Crime Act.

omission constituting an offence under this Act has been committed wholly or in part – (a) within the territory of the Kingdom of Lesotho; or (b) on a ship or aircraft registered in the Kingdom of Lesotho; or (c) by a national of the Kingdom of Lesotho outside the jurisdiction of any country; or (d) by a national of the Kingdom of Lesotho outside the territory of the Kingdom of Lesotho, if the person's conduct would also constitute an offence under a law of the country where the offence was committed". It acknowledges that electronic evidence is admissible in the courts of law.

It also provides a set of procedural instruments necessary to investigate cybercrime such as the protection of integrity of computer data during an investigation. The Bill empowers a judge or magistrate with authority to "issue a warrant authorising a [law enforcement or police officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access: (i) a computer system or part of it and computer data stored therein; and (ii) a computer-data storage medium in which computer data may be stored".

Unlike other pieces of legislation on cybercrime, the draft Bill points out that the internet service providers have no obligation to monitor data "which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity". As a result, this clause limits the liability of internet service providers to criminal liability. This is important for the protection of the right to privacy as enshrined the Constitution of the Kingdom of Lesotho.

Malawi

Malawi's Electronic Transactions and Cyber Security Act came into effect in 2016. The objectives of the law are to "to make provision for electronic transactions; for the establishment and functions of the Malawi Computer Emergency Response Team (MCERT); to make provision for criminalizing offences related to computer systems and information communication technologies; and provide for investigation, collection and use of electronic evidence; and for matters connected therewith and incidental thereto". Section 2 of the Africa defines "computer system" as "a device or a group of interconnected or related devices, one or more of which performs automatic processing of data pursuant to a program". As such, this particular definition corresponds with the definition under the Budapest Convention. Under section 92 of the Act, "hacking" refers to, "Any person who hacks into any computer system...commits an offence"" Section 87(3) of the Act punishes any person who "intercepts any data without authority or permission to do so." Interestingly, there is no statutory definition of the term "intercept" in the Act. The criminalisation encompasses issues such as recording, listening to or monitoring of the content of a computer communication, as well as the procuring of the content of data. The interception must be done to data during its transmission to, from, and within a computer system.

The Act defines a data controller as "a person who, acting either alone or in common with other persons, determines the purpose for which, and the manner in which, any personal data is processed, or is to be processed and thus, controls and is responsible for the keeping and using of personal data, and the term includes a person who collects, processes or stores personal data". It also explains data subject as "a person from whom data relating to that person is collected, processed or stored by a data controller". The Act acknowledges the admissibility and evidential

weight of electronic messages in a court of law. Part IV of the Act deals with liability of online intermediaries and content editors and protection of online users. It sets out parameters for freedom of expression and its limits within the broad area of online political communication. It prohibits child pornography; incitement on racial hatred, xenophobia or violence; unlawful disabling a computer system, spamming, illegal trade and commerce, offensive communication, attempting, aiding and abetting crime and justification for crimes against humanity. According to the law, "a person who violates any provision of this Act, whose penalty has not been provided, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and up to seven years imprisonment." This section also seeks to promote human dignity and pluralism in the expression of thoughts and opinions; protect public order and national security; facilitate technical restriction to conditional access to online communication; and enhance compliance with the requirements of any other written law. It also prohibits the production and circulation of misleading advertisements. It also outlaws unsolicited communications. It says, "a person shall not send unsolicited electronic communication to a consumer without obtaining the prior consent of the consumer".

According to the Act, "a person who provides encryption services shall declare to the Authority[7] the technical characteristics of the encryption means as well as the source code of the software used". It also gives the Malawi Communications Regulatory Authority (MACRA) the power to appoint cyber inspectors. Part VII deals with data protection and privacy. It allows for the "processing of data fairly and legally; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and processed. (e) every reasonable step shall be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, is erased or rectified; and (f) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed".

Like in Botswana, section 87(4) of the Act punishes any person who "interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective." The person must act "intentionally and without authority to do so". The Act has two offences relating to system interference. Section 87(8) (b) seeks to punish any person who "introduces or spreads a software code that damages a computer, computer system or network." This code includes viruses, worms, Trojan horses, logic bombs, bots, root kits and back doors. Section 93 punishes "any person who willfully or maliciously renders a computer system incapable of providing normal services to its legitimate users." In practice, this criminalisation is not limited to an interference caused by the inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data as required under the Budapest Convention.

Namibia

Like Malawi, Namibia first introduced a two-in-one law under the title Electronic Transactions and Cybercrime Bill in 2017. The Bill received widespread criticism from various stakeholders, which forced the Ministry of Information,

7The Malawi Communications Regulatory Authority as established under section 3 of the Communications Act.

Communication and Technology to withdraw the Bill from the public consultation processes. Media reports suggest that the revised Cybersecurity and Cybercrimes Bill will be presented to parliament towards the end of 2020. These reports suggest that unlike the two-in-one Bill presented in 2017, various separate laws dealing with a number of interconnected issues such as data protection, electronic transactions, cybersecurity and cybercrimes will be tabled before the House of Assembly. At the time of its presentation in 2017, the Electronic Transactions and Cybercrime Bill was criticized for failing to define key terms such as cybercrime, cybersecurity, functionary, forensic tools, access, data, privacy, seize and so forth. Concepts such as 'computer system' were under-defined despite the specialized and technical nature of their usage in the field of cybersecurity and data protection. The Bill also received criticism for failing to deal in a structured and substantially consequential way with the necessary aspects of combatting cybercriminal activities (IPPR and Action Namibia, 2017). Generally, it lacked coherence.

Building on part 6 of the Communications Act of 2009, the proposed Bill sought to enable warrantless search and seizure operations, while other sections seem to allow for a system of secret warrants and unauthorised access by state agents. For instance, chapter 5, in sections 43 (2) and (3), seems to enable unauthorised access and access without notification by the Communications Regulatory Authority of Namibia (CRAN) and others to computer systems, which in actual fact amounted to government hacking of private computer systems. Another questionable provision is chapter 7, in section 61 (6), (7) and (8), which grants a 'Computer Security Inspector' the power to access computer systems without giving notification or seeking legal authorisation. This raises the question of legality. Sections of chapter 8, in sections 70 (2) and all of section 72, allow for a system of secret warrants while vaguely defining the conditions under which such secret warrants can be sought. These provisions open the door to pervasive communications surveillance and interception without appropriate oversight mechanisms to monitor the conduct of those carrying out such surveillance or interception activities (IPPR and Action Namibia, 2017). It was drafted in such a way that unauthorised access by state agents and interception of communications was under regulated.

The proposed Bill made no provision for a 'designated judge' to hear interception applications. This kind of an oversight mechanism has the potential to foster transparency and accountability in the state security value chain. Thus, a system of secret warrants and warrantless accessing of private data and communications and computer systems, which the Bill wanted to smuggle into the public domain violates the necessary and proportionate principles. In order to curb the excesses of part 6 of the Communication Act of 2019, the proposed Bill must endeavor to establish an independent oversight mechanism to ensure transparency and accountability of communications surveillance. Concerns are rife amongst human rights defenders that Namibia engages in illegal communications surveillance even though part 6 of the Communication Act has not yet been operationalised.

Another borne of contention was the lack of data and privacy protections. The proposed law did not adequately provide for personal data protection or proscribe the rights of data subjects, in line with necessary and proportionate principles. The Bill was also silent on procedures to be followed by state officials when examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from the interceptions. Given that the right to privacy is explicitly enshrined in the Namibian

Constitution, the absence of substantive personal data and privacy protections in the proposed law ignited substantial constitutional questions. Civic groups such as the Namibia Action Coalition Namibia Trust and IPPR have called for the inclusion of user notification provisions in the revised Bill. Under chapter 5 dealing with accreditation of security services or products, the Bill attempted to introduce a rather onerous and intrusive registration regime, appears throughout to enable state agents to establish and open "backdoors" in encryption technologies. This is despite scholarly evidence suggesting that anonymity-granting technologies and end-to-end encryption provide the security and privacy necessary for exercising fundamental human rights online and for individuals, businesses and governments to engage activities that support economic growth and social progress.

Issues like lack of transparency and access to information and excessive and unaccountable ministerial power have also been highlighted as sticking points. The draft law does not explicitly encourage access to information. Although Chapter 6, which addresses the liability of service providers for processing data, the Bill has limited transparency-inducing measures, and does not in any way compel government authorities, law enforcement or private companies to account for their actions openly. This is incompatible with the AU Convention on Cyber Security and Personal Data Protection. The Bill invests discretionary decision-making and appointing power in the minister. It does not include oversight or accountability measures with regard to ministerial conduct.

South Africa

South Africa has also not escaped the bandwagon of coming up with the Cybercrimes and Cybersecurity Bill. On 9 December 2016, the country gazetted the Bill modeled along the SADC Model Law. It seeks to "create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which is harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes; to provide for the establishment of structures to promote cybersecurity and capacity building; to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; to provide that the Executive may enter into agreements with foreign States to promote cybersecurity; to delete and amend provisions of certain laws; and to provide for matters connected therewith." Despite the initial enthusiasm that accompanied the introduction of the Bill in the House of Assembly, four years have passed without its passage into law. The Act punishes the following cybercrimes: unlawful securing of access, unlawful acquiring of data, unlawful acts in respect of software or hardware tool, unlawful interference with data or computer program, unlawful interference with computer data storage medium or computer system, unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices, cyber fraud, cyber forgery and uttering, cyber extortion, aggravated offences and attempting, conspiring, aiding, abetting,

inducing, inciting, instigating, instructing, commanding or procuring to commit offence. In terms of penalties, any person who contravenes the provisions of the Act is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment.

Section 3 of the Act defines "unlawful acquiring of data" as "any person who unlawfully and intentionally overcomes any protection measure which is intended to prevent access to data; and acquires data, within or which is transmitted to or from a computer system, is guilty of an offence. Section 16 of the Act stipulates that "any person who unlawfully makes available, broadcasts or distributes, by means of a computer system, a data message to a specific person, group of persons or the 5 general public with the intention to incite— (a) the causing of any damage to any property belonging to; or (b) violence against, a person or a group of persons, is guilty of an offence". The burden of proving the "intent to incite" is very complicated. Similarly, section 18 of the Act, which deals with revenge pornography is too broad. Negligence should be sufficient to be convicted of unlawfully distributing revenge porn as many people argue they did not intend to distribute revenge porn. It is difficult to establish the legal requirement of intention. Besides the issue intention, both sections have key concepts such as "broadcasts" and "distributes", which are not clearly defined. For instance, the definition of "data message" in the proposed Bill is different from the Hate Crimes Bill. This confusion over key definitions opens room for the misuse of the provision. It violates the freedom of expression as outlined in section 16 of the South African Constitution, which only excludes expression that leads to "incitement of imminent violence". Some of the expressions explicitly outlawed by the South African Constitution include: propaganda for war, incitement of imminent violence and advocacy of hatred based on race, ethnicity, gender or religion, which constitutes an incitement to cause harm.

Unlike similar laws in the region, the proposed Bill requires more stringent conditions to be met before a warrant is issued. However, sections 29 and 30 allow for the warrantless search and seizure of computer devices under certain circumstances. This means that the courts are left with the onerous role of demarcating the reasonable grounds within which warrantless searches and seizures may be carried out without unnecessarily and illegally violating a citizen's privacy. In many ways, the Bill can be viewed as an adopted and improved version of SADC Model Law. This does not mean the Bill is without its own challenges. The Bill has been criticized for attempt to limit the free flow of communications through its opaque and broad definitions of 'data message'. Section 17(2) (d) refers to messages which are "inherently false in nature". There are no objective criteria to determine what this means. The causing of "mental, psychological or physical harm" is taken from the Harassment Act. The Bill thus alters the definition of what is harmful in data messages. This is an overbroad limitation of freedom of expression.

Section 38 of the Bill expands on the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), which has been singled out as granting state security agencies with excessive power to conduct surveillance on citizens, investigative journalists and political opponents. For instance, RICA does not provide for notification of interception orders to affected parties. This means the legality of such an order cannot be reviewed because no notification of

this order is communicated. Section 37 of the Bill reiterates RICA's prohibition on disclosure. Section 38(3) (b) (i)-(iv) deals with obligations of communication service providers. This section requires service providers to store information of clients but makes no differentiation for different categories of information. The vagueness of the requirement unduly limits the constitutional right to privacy. Key informants have proposed that blanket provisions on disclosure and information sharing should also be reviewed. This is very important in light of section 14 of the Constitution, which protects the right to privacy. This includes the right not to have the privacy of one's communications infringed.

Key informants in this study raised concern about certain provisions which are overbroad and vague. Other provisions provide too much power to state security agencies. Concerns have been raised about particular provisions, which are framed in ways that suggest that they want to regulate harmful expression but can easily be used to limit freedom of expression. The Bill has provisions inhibiting the production and circulation of misleading and false news and information. A closer reading of the Bill suggests that the State would like to assume the position of the final arbiter what is deemed as truth or non-truth. This can easily be abused to limit freedom of expression and digital activism. Respondents advocated for the establishment of a civilian body, which can ensure the powers granted to state security in the Bill are not abused. Equally problematic is the part of the bill, which addresses the issue of information sharing. The provision requires the Minister of Justice to make regulations on data sharing. It is not clear how the information will be stored. In the proposed Bill, there is no provision made for the destruction of intercepted data after a certain period.

Tanzania

Tanzania gazetted its Cybercrime Act in May 2015. On close reading, it is clear that the legislation borrows from the SADC Model Law. Consequently, it has transplanted all the privacy-infringing provisions of the SADC Model Law into its national legislation. Ever since it was passed, the Act has been (ab)used by the government to arrest citizens that used online media to express criticism of President Magufuli. In this regard, the Cybercrime Act is perceived more as a tool to oppress the freedom of expression and the closely related right to privacy. Similar to the SADC Model Law, the Cybercrime Act grants the police force and State security agencies excessive powers when investigating alleged cybercrimes. It's couched in broad and vague language, which can easily be abused to criminalise online communications. An example is section 4 of the Act, which defines the offence of illegal access as follows, "...person shall not intentionally and unlawfully access or cause a computer system to be accessed." A person commits the offence by either accessing a computer system, or causing a computer system to be accessed by another person. Here, the term "access" is defined in section 2 of the Act as meaning "entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system or network or data storage medium".

Section 6 of the Act criminalises the interception of data or communication by technical means or by any other means (i) a non-public transmission to, from or within a computer system; (ii) a non-public electromagnetic emission from a computer system; (iii) a non-public computer system that is connected to another computer system. The interception must be "intentionally and unlawfully". The Act defines "interception"

as encapsulating "acquiring, viewing, listening or recording any computer data communication through any other means of electronic or other means, during transmission through the use of any technical device." Although some of the wording in this section is problematic, it borrows heavily from the Budapest Convention. Section 7 of the Act makes it an offence for any person who (a) damages or deteriorates computer data; (b) deletes computer data; (c) alters computer data; (d) renders computer data meaningless, useless or ineffective. The person commits the offence if he or she acts intentionally and unlawfully. The definition also captures the elements of the offence as required by the Budapest Convention.

The Act has been used to arrest social media users and bloggers in Tanzania. Given the broad and vague definitions of some of the offences that criminalised under the Act, it was noted that the government of Tanzania have abused the law to silence critics and dissent.

Zambia

In August 2018, the Zambian government approved the Cyber Security and Cyber Crimes Act, which seek to regulate social media and enhance cyber security. It replaced the Electronic Communications and Transactions Act of 2009. The main objectives of the Act are to: (a) authorise the taking of measures to ensure cyber security in Zambia; establish the Zambia National Cyber Security Agency and provide for its functions; protect victims against cybercrime; provide for Child Online Protection; provide Information and Communication Technology user education on cybersecurity and develop local skills in cyber security; facilitate identification declaration and protection of critical information infrastructure; repeal certain provision in the Electronic and Communications Transactions Act No. 21 of 2009; provides powers to investigate and prevent cybersecurity incidents, criminalise offences against computers and network related crime; provide for investigation and collection of evidence for computer and network related crime; provide for the admission of electronic evidence for such offences; and provide for matters connected within or incidental ton the foregoing.

The Act also deals with various crimes committed using internet and social media platforms. It deals with issues such as extradition, admissibility of electronic evidence, search and seizure, collection of traffic data, interception of content data and mutual assistance and cooperation relating to the investigation and prosecution of an offence committed under the Cyber Crime Act. It seeks to facilitate intelligence gathering, investigation, prosecution and judicial processes in respect of preventing and addressing cybercrimes, cyber terrorism and cyber warfare. However, progressive civic groups such as MISA-Zambia and Zambian Bloggers Network have argued that this Act has several provisions that have the potential to infringe on internet freedoms. For example, the Act provides penalties of up to one year in prison, fines, or both for "any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person," which could be used to crackdown on legitimate online expression.

The Act also facilitates the establishment of a cyber security regulator, which seeks to protect Zambia's critical infrastructure from cyber-attacks. The regulator is the Zambia Cyber Security Agency. Some of the functions of the agency include: (a) coordinate the Zambia Computer Incidence Response Team; coordinate and oversee all activities related to cybercrime

and cybersecurity; develop and promote an all-inclusive secure cyber ecosystem; create a safer cyber space in Zambia; coordinate the protection of Zambia's critical information infrastructure; establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure; promote, develop, maintain and improve competencies and expertise and professional standards in the cybersecurity community; and promote research and development the use of new and appropriate technologies and techniques in cyber security and cybercrimes and so forth.

However, the board of the agency consists of a representative each from the following security wings: (i) the Zambia Air force; (ii) the Zambia Army; (iii) the Zambia National Service; (iv) the Zambia Police; and (v) the Zambia Security Intelligence Services; (b) a representative from the Ministry responsible for communications; (c) a representative from Engineering Institute of Zambia; (d) a representative from the Law Association of Zambia; and (e) one other person appointed by the Minister with experience in cyber security. This raises issues about the independence of the oversight mechanism, which opens up the whole exercise to intrusive surveillance under the guise of promoting cybersecurity.

With regards to power to inspect, search and seize, the Act grants a cyber inspector the power "to monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity to the appropriate authority; in respect of a critical information infrastructure and perform an audit". It prohibits the disclosure of intercepted communication. Section 46 of the Act calls upon internet service providers to ensure that they use electronic communications systems that are technically capable of supporting lawful interceptions; install hardware and software facilities and devices to enable the interception of communications when so required by a law enforcement officer or under a court order; provide services that are capable of rendering real-time and full-time monitoring facilities for the interception of communications; provide all call-related information in real-time or as soon as possible upon call termination. The Act stipulates that, "any service provider who fails to comply with the requirements of subsection (1) commits an offence and is liable upon conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years or to both". This provision violates the right to privacy as enshrined in the Zambian Constitution.

Besides the Cyber Security and Cyber Crimes Act, the Electronic Communications and Transaction Act of 2009 provides for the protection of personal information and details conditions for the lawful interception of communications, though several provisions give the government sweeping surveillance powers with little to no oversight. For instance, Article 79 requires service providers to enable interception and store call-related information. Article 77 requires service providers to install both hardware and software that enable communications to be intercepted in "real-time" and "full-time" upon request by law enforcement agencies "or" under a court order. Internet intermediaries are also required to transmit all intercepted communications to a Central Monitoring and Coordination Centre managed by the communications ministry. Internet intermediaries that fail to comply with the requirements could be held liable to a fine, imprisonment of up to five years, or both.

These provisions violate the right to privacy and freedom of expression.

Since 2016, Zambia has witnessed infringements on internet freedom. Several individuals have been arraigned before the courts on charges of defamation against the president (Freedom House, 2019). Government officials have periodically issued chilling threats against social media "abuse." In this regard, fake news, cyber-bullying, and other computer-based "crimes" have been identified as threats to national security. The government has proposed the "China way" and Ethiopia as models for dealing with the internet, threatening to ban Facebook, Google, and other social media sites to curb their abuse. In May 2019, Zambia's regulatory authority announced new rules requiring WhatsApp group administrators to register their WhatsApp groups and create a code of ethics, or risk arrest. If enforced, the rules could lead to proactive censorship and increased self-censorship (Freedom House, 2019). These regulations have been seen as part of the broader agenda by the government to control online speech.

Zimbabwe

Since 2013, the country has been working on the cybersecurity and cybercrimes legislation. The bill has had many false starts along the way. It has been given various names including the initial Computer Crimes and Cybersecurity Bill and now the Cyber Security and Data Protection Bill. Although the Bill claims that it pays particular attention to the Constitution of Zimbabwe, international standards, and comparable statutes from other jurisdictions, it is important to note that it borrows extensively from the SADC Model Law. It also leans heavily towards the Tanzanian Cybercrime Act. Like the Tanzanian government, the Zimbabweans government has conveniently used the guise of investigating cybercrime to prosecute citizens that express anti-government sentiment online (Hove, 2019). The Cybersecurity and Data Protection Bill's main objective is to increase cybersecurity in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects. It stipulates this as follows:

The purpose of this Bill is to consolidate cyber related offences and provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest, to establish a Cyber Security Centre and a Data Protection Authority, to provide for their functions, provide for investigation and collection of evidence of cybercrime and unauthorised data collection and breaches, and to provide for admissibility of electronic evidence for such offences. It will create a technology driven business environment and encourage technological development and the lawful use of technology.

The gazetted Bill has converged two related issues of cybersecurity and data protection into one piece of legislation. There are concerns that the Bill will be used to push a narrow agenda focusing on protection of 'national interests' and the prevention of 'social media abuse' at the expense of digital security and protection of the privacy of internet users in Zimbabwe (MISA, 2020). For instance, Section 5 and 7 of the Bill seek to designate the Postal and Telecommunications Regulatory Authority of Zimbabwe (established in terms 30 of the Postal and Telecommunications Act [Chapter 12:05]) (POTRAZ), as the Cybersecurity Centre and Data Protection Authority, respectively. This means that POTRAZ will become a converged regulatory body: the regulator of the telecommunications industry, the cybersecurity centre and the data

protection authority. Whilst the convergence of regulatory authorities may help the government to save on financial resources, it defeats the principle of separation of powers and check and balances, which are critical in the era of "data deluge". Furthermore, this convergence can foster unnecessary operational inefficiencies. In order to remedy the situation, key informants observed that there is need for the equal prioritisation and balancing of the functions of the Cybersecurity Centre and Data Protection Authority to ensure that significance is not placed only on cybersecurity while data protection, privacy and the interrelated fundamental rights are neglected. The conflation of these three institutions poses a dual crisis, with POTRAZ, on one hand, becoming the surveillance arm of the state while also having access to the large volumes of data collected by the Mobile Network Operators (MNOs) and Internet Service Providers (ISPs). This, therefore, compromises data protection and the right to privacy.

The Bill makes provision for the processing of data, which can be done by telecommunication operators, electronic management bodies, ministry of home affairs and other immigration agencies. It stipulates that data processors must notify the data subjects before the collection of the information as well as how the data will be processed. The Bill criminalises the processing of sensitive information, genetic data, biometric data and health data. It is only allowed under specified circumstances, which include where the processing is necessary to comply with national security laws and also for the prevention of imminent danger or the mitigation of a specific criminal offence. The Zimbabwe's Cybersecurity and Data Protection Bill is an omnibus law combining cybersecurity and data protection (MISA-Zimbabwe, 2020). This is partly because it borrows heavily from the African Union's model law. In view of this amalgamation of two separate but mutually related issues (cybersecurity and data protection), civil society groups have called for the drafting of two separate laws.

Although the Bill does not explicitly mentions the issue of intrusive communications surveillance, there are several pieces such as the Official Secrets Act, Criminal Law (Codification and Reform) Act and the Interceptions of Communications Act, which have been used to justify the snooping on citizens' online communication. Some of these laws were passed before 2013 hence have not yet been aligned with the Constitution. In circumstances where information relates to national security, more often than not, there is no disclosure of sufficient information under the auspices of national interests. This poses the danger of such provisions being abused and exposing citizens to over surveillance by government and state security agents, thus, violating their right to privacy. In the event of any security breach, the Bill provides in Section 19, that the data controller shall notify the Authority, without any undue delay of any security breach affecting data that he or she processes. It is imperative that the law should provide a specific timeline under which the security breach shall be communicated rather than leaving the provision open to interpretation on what entails undue delay. In addition, the Bill provides an obligation to data controllers, except for those in specified circumstances to notify the Data Protection Authority prior to any wholly or partly automated operation or set of operations intended to serve a single purpose or several related purposes.

The notification is not required where the data controller has appointed a data protection

officer[8] . It is also important for the law to make it obligatory for every data controller to appoint a data protection officer. However, the question that therefore arises is who polices the data protection officer and ensures that they are independent and exercise due diligence? The Bill also amends the provisions in Sections 163-166 of the Criminal Law (Codification and Reform) Act, which speaks on offences relating to computer systems, computer data, data storage mediums, data codes and devices. The Bill has provisions for dealing with offenses related to hacking, unlawful interference and interception of data and computer systems. It should also be noted that the Internet has created a global village and such hacking or unlawful interferences can be perpetrated by persons outside Zimbabwe and thus outside the jurisdiction of our law enforcement authorities.

There are, however, other provisions that have the potential to infringe on the exercise of media freedom, freedom of expression and access to information. For instance, section 164 states:

> "Any person who unlawfully by means of a computer or information system makes available, transmits, broadcasts or distributes a data message to any person, group of persons or to the public with intend to incite such persons to commit acts of violence against any person or persons or to cause damage to any property shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment."

Like insult laws, the above provision can easily be used to inhibit constructive criticism, which is important for promoting transparency and accountability especially from the government. In a context of polarized politics and retribution, such provisions can be used as political tools and mechanisms by the state to prevent the expression of dissenting opinions. In the end, such a provision can contribute immensely towards stifling citizen engagement and open debate, which are essential building blocks for electoral and constitutional democracy.

Under section 164B, the Bill criminalises not only the production but also the communication of offensive messages from 'any electronic medium accessible by any person', which in essence also includes social media. This relates to cyber-bullying and harassment. Section 164C of the Bill deals with mis-and disinformation. It criminalises the use of a computer or information system to avail, broadcast, distribute data knowing it to be false and intending to cause psychological or economic harm to someone, also seems to be targeted against the spread of false information on social media. This raises a number of issues in terms of measuring the intentional production and circulation of false and misleading information in order to cause harm. It also assumes that the "arbiter of truth" can easily be identified. This clause ignores the fact that there are multiple truths and various regimes of truth and non-truth. Even more important it ignores the fact that on the internet and social media platforms it difficult to determine the origin and authenticity of a message. In such an environment, individuals are exposed to communication messages voluntarily or involuntarily. In a context, where a culture of citizen journalism and blogging has taken route, this provision can be abused to implicate thousands of ordinary citizens who would have 'received' and communicated such messages.

Cognisant of the dangers that lurks in the woods,

8A data protection officer in terms of the Bill, refers to any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in this Bill.

civil society organization have proposed the outlining of clear procedures and elements in order to establish intention to commit the offences so as to ensure that a balance will be struck between regulation of the Internet space and exercise of fundamental rights (MISA-Zimbabwe, 2020).

Advocacy strategies that can be relied on to ensure that these laws promote rather than curtail the exercise of rights

This section foregrounds advocacy strategies that can be used to inform the necessary interventions that should be done to promote the human rights-based approach in the coming up with data protection, cybersecurity and cybercrimes, and electronic transactions legislation in the region. It was noted by the respondents that there is need to engage in strategic litigation, capacity building, research, popularisation, influencing policy and laws and advocacy linked to Model Laws and the Declaration on Principles of Freedom of Expression and Access to Information in Africa.

Key informants pointed there is urgent need to focus on advocacy around domestic laws (Cybsecurity and cybercrime laws), Model Laws (Budapest, Malabo and SADC) and the Declaration on Principles of Freedom of Expression and Access to Information in Africa. This advocacy campaigns can focus on the protection of privacy and personal information online and communication surveillance, advocacy around the Internet as a standalone right (and not advocate it under other rights), and advocacy on evaluating laws around COVID-19 for compliance with the Declaration on Principles of Freedom of Expression and Access to Information in Africa.

Another area requiring concerted efforts relates to advocacy on publicity and visibility of the domestic laws, Model Laws and the Declaration on Principles of Freedom of Expression and Access to Information in Africa. This entails popularizing the ACHPR Principles on Freedom of Expression and conduct advocacy around the instrument itself in different SADC countries, and engaging the special rapporteur on Freedom of Expression to meet different stakeholders including government officials and departments.

Another advocacy strategy, which was mentioned by key informants relate to advocacy on domestic laws, Model Laws and the Declaration linked to African Commission on Human and People's Rights activities. This encapsulates putting pressure on national governments in the SADC region to do the reporting or to do their own shadow reporting on their compliance with the Declaration and Model Laws. This is particularly important because State Parties have an obligation to also report on the Declaration in periodic reports to ACPHR. CSOs in SADC have to engage the ACPHR when there are human rights violations taking place so that it can be used to send urgent appeals or delegations to the affected countries to protect lives.

Research was also mentioned as an important strategy that CSOs and academia can use to ensure that cybersecurity and cybercrime laws are used to promote rather than curtail the exercise of inalienable rights. This consists of studies on the impact of surveillance and cyber-security laws on the protection of privacy and personal information, research on national emergency laws criminalising the spread of false and misleading information in the SADC region, research on the impact of contact tracing on the protection of privacy and personal information, comparative research on the criminalisation of racist or xenophobic hate speech, and organising sharing sessions involving the special rapporteur and parliamentarians and CSOs.

Our key informants observed that there is need for CSOs to invest heavily on understanding the provisions of domestic laws, Model Laws and the Declaration. This can take the form of holding capacity building workshops around cybersecurity and cybercrime issues and their impact on digital rights. The use of popular, traditional and digital media to popularise model laws and national legislation on cybersecurity and cybercrimes was also emphasised.

Strategic litigation was also mentioned as one of the options, whereby public interest lawyers are engaged to test the constitutionality of certain problematic provisions of the enacted and proposed legislation. Some of the possible advocacy strategies include: lobbying parliamentarians to amend problematic provisions of the cybersecurity and cybercrime laws, showing of solidarity when digital rights violations occur and using Model Laws and the Declaration in such campaigns, advocacy by CSO to demand from government and telecommunication companies' transparency reports on throttling of the Internet and Internet shutdowns, advocacy by CSOs, advocacy by CSOs to demand from data controllers and processors transparency reports on search warrants requested and issued

Recommendations

Recommendations of this report are proffered at the level of regional, sub-regional body, national governments, civil society organisations, media and academia. In short, the main thrust of the section is to underscore the need for state and non-state actors to ensure cybersecurity and cybercrime legislation is used to promote freedom of expression and right to privacy.

African Union

It is equally important to ensure that the enacted and proposed domestic laws of Southern African countries are aligned with the AU model Law on Cyber Security and Personal Data Protection and the African Declaration on Internet Rights and Freedoms.

Member States must not simply "copy and paste" the full name of the Model Law without domesticating it to their own context. Rather it is imperative for them to draft separate laws dealing with cybersecurity and cybercrime on the one hand and data protection on the other hand.

Member states must strive to fulfill the full import of Article 25 of the Convention, which calls upon State Parties to ensure that proposed or enacted cybersecurity and cybercrimes laws do not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

Southern African countries must adhere to the principles governing the processing of personal data as enumerated in Article 13 of the AU Model Law. These include: consent and legitimacy of personal data processing, lawfulness and fairness in personal data processing, purpose, relevance and storage of processed personal data, accuracy of personal data, transparency of personal data processing, and confidentiality and security of personal data processing.

SADC

Instead of adopting a wholesale "cutting and pasting" of the SADC Model Law, member states must endeavor to cherry pick the most progressive provisions that speak to their peculiar context. For instance, section 25 of the Model Law, which address issues related to search and seizure of electronic equipment suspected to have been used to commit an offence or suspected to contain information proving the commission of an offence has been critiqued for infringing on the right to privacy.

Article 25 of the Model Law must be amended in order to promote and protect the right to privacy in the digital age.

National Governments

There is need for countries in SADC region to adopt a Human Rights-Based Approach. Such an approach will ensure that the enacted or proposed legislation take into account the urgent need to balance cybersecurity needs with the need to protect and promote the fundamental right to privacy. This can be done through integrating international human rights system norms, principles (necessary and proportionate principles) and standards (model laws) and goals.

Member States must ensure that cybersecurity and cybercrime laws are aligned with national constitutions. These laws must endeavor to promote the right to privacy and freedom of expression. There is need to ensure cybersecurity

and cybercrime laws strike a balance between the protection of national security and exercise of the rights of ordinary citizens.

There is need to adhere to the Necessary and Proportionate Principles when coming up with cybersecurity and cybercrime, data protection and electronic transaction laws in the SADC region.

Public consultation processes in the coming up with cybersecurity and cybercrime legislation must follow clearly laid out procedures. Input from marginalised and vulnerable constituencies must be taken on board. Any cybersecurity law and institutional framework be the product of an extensive and meaningful cooperative multi-stakeholder consultative process and that the eventual frameworks make provision for some level of multi-stakeholder oversight involvement.

There is need to desist from coming with an omnibus type of legislation as evidenced in Malawi, Zimbabwe and Namibia. Instead of lumping cybersecurity and data protection issues together, it is recommended that the proposed Bills must be separated into two Bills that deal with cybersecurity and data protection separately in line with international best practice and instruments such as the SADC Model Law on Data Protection, African Convention on Cybersecurity and Data Protection.

Enacted and proposed legislation must ensure that there is a clause that guarantees the protection of whistleblowers in terms of handling investigations. In order to strengthen the protection framework, all protection arrangements should include a legal obligation for public officials to report misconduct and/or procedures for protecting whistleblowers and enforcing fair treatment after a disclosure has been made.

There is need to come up with independent national regulatory authorities rather than using existing bodies as would limit the effectiveness, efficiency and independence of the Board since it is appointed by and reports to the Executive. A case in point is the Zambian scenario where a separate entity (Cyber Security Centre) was created.

Cybersecurity and cybercrime laws must not be used as a smokescreen to normalise arbitrary, disproportionate and unnecessary surveillance of citizens without regard to citizens' right to privacy.

These laws must clearly define the term data subject. The rights of the data subject must be derived from the Bill of Rights in the Constitution. He/she must also be afforded the right to request a record or description of the personal information about the data subject being held by a data processor, as well as information concerning the identity of all third parties who have had access to the data subject's personal information.

The obligation of the data controller in terms of safeguarding the security, integrity and confidentiality of the data must be clearly spelt out in any proposed legislation. The clause on data controllers must ensure that they collect only the data absolutely necessary for their purposes, and access to personal data should be limited to only those necessary for processing.

Legislation on cybersecurity and cybercrime must ensure that there are adequate accountability or oversight mechanisms on data breaches. Rather than placing the duty to report on the national Cybersecurity Centre, the law must ensure that the data subject must also be given the duty to report in cases of data breaches. This clause will offer adequate protection or recourse for potential victims of breaches emanating from the Data Controller's negligence or incompetence. The law must spell out consequences for avoidable breaches e.g. by providing compensation to a data subject whose information was not adequately

protected.

National governments are encouraged to clearly define key terms and offences, which are being criminalised. It is important that countries must draft their cybersecurity and cybercrime legislation with sufficient clarity and specificity so as to ensure that they provide adequate foreseeability and guidance on the type of conduct being criminalised. It is important that the definition of offences must communicate clearly and precisely the conduct being criminalized and the applicable mental elements.

Civil Society Organisations

Need for strategic litigation focusing on problematic provisions of the legislation on cybersecurity and cybercrimes.

CSOs must commission evidenced-based research, which can be used for lobbying and advocacy related to amendments of certain provisions of the law.

Public education campaigns and awareness raising workshops on the provisions of the enacted and proposed legislation.

Publication of shadow reports and policy briefs on best practices as espoused in international, regional and sub-regional Model Laws and other best practices.

Transparency reports by data controllers and processors as well as internet intermediaries.

Media

Media organisations must continue to popularise Model Laws, international instruments and best practices and national legislation on cybersecurity and cybercrimes.

Academics and Research Institutes

There is need for academics and research institutes to invest their energy in policy relevant research that feeds into the drafting of progressive legislation.

CONCLUSION

This report has looked at enacted and proposed cybersecurity and cybercrime laws in the SADC region and how they have impacted the exercise of rights more specifically, the right to privacy, freedom of expression and media freedom. It has critically examined how these laws contravene provisions of the European Union, African Union, and SADC Model Laws. It has provided an overview of how the internet space has impacted the exercise of rights; highlight regional and international legal frameworks on cybercrimes and cybersecurity and the key principles highlighted therein for the protection and promotion of rights. It analysed cybersecurity laws in the Southern African region and how they impact the exercise of rights in countries such as Botswana, Lesotho, South Africa, Namibia, Zimbabwe and Zambia. Some SADC countries have already used the Budapest Convention as a model for developing their domestic legislations on cybercrime. The legislations of Mauritius, Botswana and Tanzania, and the draft legislations of Lesotho and South Africa are clearly premised on the Convention. This study which relied heavily on desktop review and key informants has demonstrated that although some countries in the SADC region have enacted cybersecurity and cybercrime laws, others are still in the process of drafting similar laws. On the one hand, countries like Botswana, eSwatini, Tanzania, Malawi and Zambia have already passed cybersecurity and cybercrime laws. On the other hand, countries such as Namibia, South Africa, Lesotho and Zimbabwe have gazetted draft legislation on cybersecurity and cybercrime. It has argued that although some of the enacted and proposed cybersecurity and cybercrime laws are modeled along international, regional and sub-regional model laws and other human rights instruments, there are a number of problematic provisions, which infringes on the right to privacy and freedom of expression. Second, while most of the enacted and proposed laws in the SADC region attempt to balance cybersecurity issues with human rights frameworks as espoused in national constitutions, there are still restrictive laws dealing with interception of communication, data protection and electronic transactions.

Third, in countries such as Zambia, Zimbabwe, Namibia and Malawi, there is deep-seated fear that existing and new legislation are already being used for surveillance purposes. For instance, South Africa uses the RICA Act to regulate the interception of communication. Zimbabwe has the Interception of Communications Act. Zambia deploys the Electronic Communications and Transactions Act of 2009. Fourth, there are concerns around broad and vague definitions of criminalised offences and key terms such keystroke, false news, race and xenophobic-related offences, modification, unauthorised access, or asymmetric cryptosystem, cyber terrorism, child pornography and cyber extortion and so forth. Fifth, inadequate oversight or accountability mechanisms over the functions of cyber inspectors, data controllers, internet service providers and ministers pose serious threats to the integrity and effectiveness of the legislation. Finally, the study has demonstrated that while some countries have made significant inroads in terms of criminalising cyber-related conduct, providing adequate procedural tools and mapping out international cooperation arrangements, others are still stuck at the 'crossroads' of indecision, procrastination and slow policy making.

References

African Union. (2013). AU Convention on Cyber Security and Personal Data Protection. Retrieved from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

African Union. (2019). Declaration on Principles of Freedom of Expression and Access to Information in Africa. https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf

African Declaration on Internet Rights and Freedoms (AFDEC). (2020). Privacy and Personal Data Protection in Africa Advocacy Toolkit. Johannesburg.

Brenner, S. W. & Schwerha, J. J. (2007-2008). Cybercrime havens: Challenges and solutions. Business Law Today, 17(2), 49-79.

Council of Europe. (2004). The Budapest Convention. Retrieved from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Electronic Frontier Foundation. (2013). The Necessary and Proportionate Principles. Retrieved from https://necessaryandproportionate.org/citations/page/5/

Freedom House (2019). Freedom in the World — Zambia Country Report. Retrieved from https://freedomhouse.org/country/zambia

Gillis, A., & Jackson, W. (2002). Research methods for nurses: Methods and interpretation. Philadelphia: F.A. Davis Company.

Government of Botswana. (2018). Cyber Crime and Computer Related Crimes Act. Retrieved from https://www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf

Government of Tanzania. (2015). Cybercrime Act. Retrieved https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf

Government of Malawi. (2016). Electronic Transactions and Cyber Security Act. https://crm.misa.org/upload/web/e-transactions-act-2016.pdf

Government of Namibia. (2017). Electronic Transactions and Cybercrime Bill. Retrieved from https://www.iwits.me/story/namibian-electronic-and-cybercrime-bill/

Government of Lesotho. (2020). Computer Crime and Cyber Bill. Retrieved from https://www.gov.ls/cyber-crime-a-risk-to-lesotho/

Government of South Africa. (2016). Cybercrimes and Cybersecurity Bill. Retrieved from https://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Government of Zambia. (2017). Cyber Security and Cyber Crimes Bill . https://www.lusakatimes.com/wp-content/uploads/2018/06/The-Cyber-Security-and-the-Cyber-Crimes-DRAFT-Bill-2017.pdf

Government of Zimbabwe. (2020). Cybersecurity and Data Protection Bill. Retrieved from http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf

Hove, K. (2017, July 8). The SADC Model Law on Computer Crime and Cybercrime: A Harmonised Assault on the Right to Privacy? https://www.linkedin.com/pulse/sadc-model-law-computer-crime-cybercrime-harmonised-assault-kuda-hove/

Hunter, M. and Mare, A. A Patchwork for Privacy: Mapping communications surveillance laws in southern Africa. Media Policy and Democracy Project. DOI: 10.13140/RG.2.2.33154.71363

Leininger, M. M. (1985). Qualitative Research Methods in Nursing. Orlando: Grune and Stratton.

Lincoln, Y. S. (1992). Sympathetic connections between qualitative methods and health research. Qualitative Health Research, 2(4), 375-391.

IPPR and Action Namibia. (2017). Submission: Draft Provisions of the Electronic Transactions and Cybercrime Bill (2017). Retrieved from https://action-namibia.org/wp-content/uploads/2017/10/ACTION-IPPR-Submission-on-ETC-Bill-June2017.pdf

Mare, A. (2020). Internet Shutdowns in Africa| State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe. International Journal of Communication, 14, 4244-4263.

Mare, A. (2018). Politics unusual? Facebook and political campaigning during the 2013 harmonised elections in Zimbabwe. African Journalism Studies, 38(2), 1–22.

MISA-Zimbabwe. (2020). Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019. Retrieved from https://zimbabwe.misa.org/wp-content/uploads/sites/13/2020/05/Cybersecurity-and-Data-Protection-Bill-entrenches-surveillance-MISA-Zimbabwe-analysis.pdf

Orji, U. J. (2015). Multilateral Legal responses to cyber Security in Africa: Any Hope for Effective International cooperation? A paper presented during the 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 105-118.

SADC. (2013). SADC Model Law on Computer Crime and Cybercrime. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

Seger, A. (2016). 'Implementation of the Budapest Convention on Cybercrime'. [PowerPoint Presentation]. Retrieved from http://www.oas.org/juridico/pdfs/cyb9_coe_cyb_oas_dec16_v1.pdf.

Wuest, J. (1995). Feminist grounded theory: An exploration of the congruency and tensions between two traditions in knowledge discovery. Qualitative Health Research, 5(1), 125–137.

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books.