

digital

SOUTHERN AFRICA

Issue No. 04

June 2024

rights

A photograph of a brick wall covered with a grid of surveillance cameras. The cameras are arranged in a regular pattern, with some black and some silver. The word 'rights' is overlaid in large, white, 3D-style letters across the top of the image. The title text is overlaid on a yellow background at the bottom right.

**Securing Digital Rights in
Southern Africa:
A Call to Action for
Stakeholders**

digital rights

SOUTHERN AFRICA

ISSUE 04

June 2024

Published in 2024 by the Namibia Media Trust
P. O Box 20783,
Windhoek, Namibia

Published in 2024 by the Association for Progressive Communications
P.O. Box 29755, Melville, 2109
Johannesburg, South Africa



Securing Digital Rights in Southern Africa: A Call to Action for Stakeholders ©
Namibia Media Trust. This work is licensed under a Creative Commons Attribution-
NonCommercial-ShareAlike 4.0 International License.

Author: Professor Admire Mare
Denhe Reruzivo Consultancy Hub

Editors: Lis Jordan
Zoé Titus

Graphic design: NauaWeb Trading

Typesetting and illustrations: Boldrin Titus





List of Acronyms

3G	Third Generation
ACHP	African Commission for Human and Peoples' Rights
ADRN	African Digital Rights Network
AIGS	AI Global Surveillance Index
AU	African Union
CCTV	Closed-circuit Television
CHR	Centre for Human Rights
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CSOs	Civil society organisations
DDoS	Distributed Denial of Service
DPAs	Data Protection Authorities
ICCPR	International Covenant on Civil and Political Rights
GSMA	Global System for Mobile Association
MISA	Media Institute of Southern Africa
NMT	Namibia Media Trust
OGBV	Online Gender-Based Violence
PIN	Paradigm Initiative
POPIA	Protection of Personal Information Act
SADC	Southern African Development Community
SLAPP	Strategic Litigation Against Public Participation
UNGPs	United Nations Guiding Principles on Business and Human Rights
UDHR	Universal Declaration of Human Rights
USAFs	Universal Service and Access Funds
ZEC	Zimbabwe Electoral Commission
ZESA	Zimbabwe Electrical Supply Authority

Table of Contents

▶ Introduction	05
▶ Conceptualising Digital Rights	07
▶ Social Context: A Brief Overview of Digital and Social Media in Southern Africa	09
▶ Methodological Approach	12
▶ Key Findings	12
A) Freedom Of Expression Online	14
B) Privacy And Data Protection	17
C) Access To Information	19
D) Cybersecurity	20
▶ Call To Action	21
Practical Advocacy Interventions	21
▶ Conclusion	22

Introduction

The mass permeation and adoption of digital technologies across the world has led to the expansion of the scope and breadth of human rights. Whereas in the past, human rights discourses centred around promoting and protecting the enjoyment and exercise of rights and freedoms in offline spaces, the advent of digital and social media platforms have necessitated a rethink of the boundaries and scope of rights more broadly¹. The blurring of online and offline spaces in contemporary societies also presupposes that rights have a broader scope than in the past.²

This rethinking of the scope and breadth of human rights has seen discussions gravitating towards an appreciation of digital rights as an extension of offline human rights³. This marks a significant shift from the traditional ways of doing things whereby citizens used to assert their positions in relation to the state by claiming human and civil rights and making rights claims⁴. In this context, the state was obligated to respect, protect and fulfil the human rights of individuals within their jurisdiction. This included the duty to protect against human rights abuse by third parties, including business enterprises. There is an acknowledgement that the triangle between the state, the market, and the citizenry requires careful balance to protect civic digital rights and liberties and to enable participation and active citizenship.

The increased power of global technology companies and social media platforms has had a direct impact on whether we really do have an equal ability to express ourselves and make political statements online.⁵ Internet intermediaries and platform companies have become important role players in the actualisation and enjoyment of human rights. At a continental level, African civil society has drafted the African Declaration on Internet Rights and Freedoms⁶ addressing the issue of how to protect human rights and freedoms on the Internet. The African Union, in 2018, adopted the Declaration on Internet Governance and Development of Africa's Digital Economy⁷.

Cognisant of their invaluable role as internet intermediaries, the United Nations drafted the "Guiding Principles on Business and Human Rights"⁸ (UNGPs), which were developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises.

The guidelines are considered to be one of the most authoritative, normative frameworks guiding responsible business conduct and addressing human rights abuses in business operations and global supply chains.⁹

In the last few years, advocacy reports, policy briefs and research papers have sought to shed light on the state of digital rights at the national, regional and continental levels. These include reports by the Centre for Human Rights (CHR) at the University of Pretoria, Research ICT Africa, ALT Advisory, Association of Progressive Communications, Collaboration on International ICT Policy for East and Southern Africa (CIPESA), and Paradigm Initiative (PIN). In 2018, ALT Advisory and Media Legal Defence Fund published a report titled, "*Mapping Digital Rights and Online Freedom of Expression Litigation in East, West and Southern Africa*."¹⁰ The report mapped the current landscape in respect of digital rights and online freedom of expression in East, West and Southern Africa. It also discussed the trends regarding law and policy developments, as well as litigation.

- 1 Musiani, F., Pavan, E, and Padovani, C. (2010). Investigating Evolving Discourses On Human Rights in the Digital Age: Emerging Norms and Policy Challenges. *International Communication Gazette*, 72(4): 1-40.
- 2 Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, 44, 1-13.
- 3 <https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights>
- 4 <https://www.coe.int/en/web/compass/what-are-human-rights->
- 5 https://digitalfreedomfund.org/wp-content/uploads/2020/12/Human-Rights_V3.pdf
- 6 <https://africaninternetrights.org/declaration/>
- 7 https://archives.au.int/bitstream/handle/123456789/8149/Assembly%20AU%20Decl%203%20XXX%20_E.pdf?sequence=1&isAllowed=y
- 8 https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
- 9 <https://www.undp.org/sites/g/files/zskgke326/files/migration/in/UNGP-Brochure.pdf>
- 10 https://www.mediadefence.org/wp-content/uploads/2020/06/Mapping-digital-rights-litigation_Media-Defence_Final-1.pdf

In 2022, the Centre for Human Rights published a report¹¹ titled “*The Digital Rights Landscape In Southern Africa*”, which sought to assess the extent to which Southern African countries have adopted laws and regulations that are in compliance with international law and standards to advance the position that the same rights that people enjoy offline should also be protected online. In September 2023, CIPESA launched the State of Internet Freedom in Africa report titled, ‘*A Decade of Internet Freedom in Africa: Recounting the Past, Shaping the Future of Internet Freedom in Africa*’.¹² The report shines light on what needs to be done to promote and protect digital rights and freedoms in a digitising continent. It also teases out the role that different stakeholders need to play to realize the Digital Transformation Strategy for Africa and Declaration 15 of the 2030 Agenda for Sustainable Development on leveraging digital technologies to accelerate human progress, bridge the digital divide, and develop knowledge societies.¹³

Extant research has shown that digital rights are under threat in Africa.¹⁴ This situation has been compounded by the weaponisation of lawfare, invasive digital surveillance practices¹⁵, coordinated disinformation campaigns¹⁶, internet and social media shutdowns¹⁷, cyber-criminal attacks and the shrinkage of the democratic space. Like elsewhere, evidence of democratic regression and creeping digital authoritarianism¹⁸ has been noted in some of the countries on the continent. Digital authoritarianism refers to the use of digital media technologies by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations.¹⁹ This has had an adverse effect on the realisation and enjoyment of digital rights and freedoms. Despite these setbacks, digital and social media platforms are still hailed as veritable sites for achieving broad-based social justice, as well as unlocking socio-political and economic freedoms. Research has pointed to diverse ways in which Africans are circumventing digital surveillance and digital authoritarianism hurdles put in their way²⁰. Besides individual users, civil society organisations and human rights defenders have been at the forefront of raising and amplifying their voices on the urgent need to promote and protect the exercise of digital rights.

In this vein, the African Digital Rights Network (ADRN) has also played a significant role in producing knowledge on the actors and technologies involved in the opening and closing of civic space online.²¹ It has also contributed towards building the capacity of citizens to exercise, defend and expand their rights online and offline.²²

This report on the state of digital rights in Southern Africa seeks to shed light on the extent to which countries are living up to the responsibility to promote and protect the right to freedom of expression, access to information, right to privacy and cybersecurity in the digital age. This is very pertinent in the context of existing national, regional and international human rights frameworks which give effect to digital rights. Building on key informant interviews and desktop research, this report highlights the positive developments associated with the passage of progressive data protection laws, setting up of data protection authorities, promotion of free expression online, amendment of access to information laws and promotion of the safety of journalists online.

11 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

12 https://cipesa.org/wp-content/files/reports/SIFA23_Report.pdf

13 <https://cipesa.org/2023/09/sifa2023/>

14 https://africaninternetrights.org/en/resource/southern-africa-digital-rights-issue-number-1-data-and-online-privacy-under-attack#:~:text=Digital%20rights%20are%20under%20threat,digital%20rights%20non%2Dgovernmental%20organisations.https://africaninternetrights.org/sites/default/files/Digital%20Rights%20Southern%20Africa_Issue%201.pdf

15 Munoriyarwa, A. And Mare, A. (2022). *Digital Surveillance in Southern Africa: Policies, Politics and Practices*, Cham: Springer.

16 Mare, A., Mabweazara, H. M. & Moyo, D. (2019). “Fake News” and Cyber-Propaganda in Sub-Saharan Africa: Recentring the Research Agenda, *African Journalism Studies*, 40:4, 1-12.

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

18 <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>

19 <https://www.populismstudies.org/Vocabulary/digital-authoritarianism/>

20 Munoriyarwa, A. And Mare, A. (2022). *Digital Surveillance in Southern Africa: Policies, Politics and Practices*, Cham: Springer.

21 <https://www.africandigitalrightsnetwork.org/>

22 <https://www.africandigitalrightsnetwork.org/>

It also critically reflects on the negative developments as evidenced by the introduction of claw back clauses around the publication and distribution of false news, passage of draconian cybercrime laws, digital surveillance practices, internet shutdowns and throttling, harassment and intimidation of journalists online, introduction of mandatory SIM Card registrations, and the imprisonment of citizens and human rights defenders for online speech. It proffers advocacy interventions that civil society groups in the region including the Namibia Media Trust (NMT), the Media Institute of Southern Africa (MISA) Regional Secretariat, Spaces of Solidarity, CIPESA, Paradigm Initiative and the Centre for Human Rights can implement to protect the realisation of digital rights in the region.

Conceptualising Digital Rights

The concept of 'digital rights' has entered the mainstream lexicon with various definitions, connotations, and interpretations. Most of the discussions have centred around what constitutes the 'digital'. In this discussion, there has been a tendency to conflate the 'digital' with online or the internet.²³ The argument is that not everything digital is always connected to the internet. For instance, biometric data, such as facial recognition and fingerprint checking are not connected to the internet but are part of the digital.²⁴ As a result, there is no consensus on what 'digital rights' mean in various jurisdictions. However, in recent years, there has been convergence around what the bundle of digital rights entails in practice.²⁵ For some, digital rights are those human rights and legal rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices, and telecommunications networks.²⁶ Digital rights are human rights online that concern access, participation, data security, and privacy, with the human-centred values of dignity, respect, equality, justice, responsibility, consent, and environmental sustainability.²⁷ Others define digital rights as human rights in the digital environment. In other words, these encapsulate human rights that are enabled through digital and social media platforms.

Digital rights are human rights online that concern access, participation, data security, and privacy, with the human-centred values of dignity, respect, equality, justice, responsibility, consent, and environmental sustainability.

These consist of the right to privacy, freedom from violence, freedom of political opinion, freedom of expression and freedom of association. It is about free speech or expression, association and assembly, access to internet devices, rights and access to information, access to platforms (such as Facebook, X (formerly Twitter), WhatsApp, TikTok, YouTube, Instagram and so forth), online safe space, security and safety, privacy and data protection, gender-responsiveness and anti-discrimination, and equality.²⁸ These rights are meant to ensure control, autonomy, and agency of humans while protecting them against the privatisation, monopolisation, and monetisation of their data and digital footprints. They ensure access to equal rights to information, technology, and knowledge; being free from violence, surveillance and discrimination; and respect privacy, autonomy and self-determination.

23 <https://www.techtarget.com/whatis/definition/digital-divide>

24 <https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-2-introduction-to-digital-rights/what-are-digital-rights/tps://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics>


25 <https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-2-introduction-to-digital-rights/what-are-digital-rights/>

26 <https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-2-introduction-to-digital-rights/what-are-digital-rights/>

27 <https://www.apc.org/en/news/coconet-what-are-digital-rights>

28 <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/>

FRAMEWORK FOR CONCEPTUALISING DIGITAL RIGHTS



1 Access to information

Internet applications and content must be transmitted without disproportionate interference or discrimination by non-state actors, including providers, for freedom to access information to be meaningful.

2 Freedom of expression online

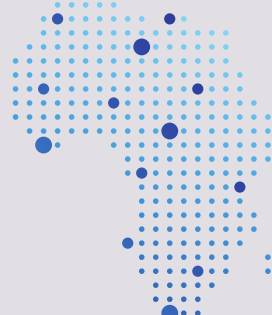
Online platforms, such as search engines, social media sites, and online forums, are becoming more prevalent fora for the expression and exchange of opinions.

3 Cybersecurity

It is imperative to safeguard internet-connected systems against cyberthreats, including hardware, software, and data.

4 Data privacy

In a society where every online action leaves a digital imprint, it becomes progressively more difficult to maintain online privacy.



In Africa, the **Declaration on Internet Rights and Freedoms** provides a comprehensive framework for promoting and protecting the exercise of digital rights. Digital rights and freedoms are assessed within the context of four parameters: **cybersecurity, data privacy, freedom of expression online and access to information.**

Although the discussion around the necessity and place of digital rights is a recent phenomenon, its articulation has a long history in international human rights law. For instance, human rights instruments under the United Nations (UN)²⁹ and in the African human rights framework affirm that the same rights people have offline should also be protected online.³⁰ Furthermore, these rights are enshrined in several foundational international law instruments,³¹ including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR),³² and the African Charter on Human and Peoples' Rights (the African Charter).³³ These rights have also been underscored by the Joint Declaration on Freedom of Expression and the Internet by the UN Special Rapporteur on Freedom of Opinion and Expression.³⁴ In Africa, the African Union's Declaration on Internet Rights and Freedoms³⁵ provides a comprehensive framework for promoting and protecting the exercise of digital rights. For the purposes of this report, digital rights and freedoms are assessed within the context of four parameters. These are cybersecurity, data privacy, freedom of expression online and access to information in selected countries in SADC (see table 1). These include countries such as Botswana, Eswatini, Lesotho, Malawi, Mozambique, Namibia, South Africa, Zambia and Zimbabwe. The main aim is to assess the extent to which these countries are upholding and protecting these digital rights and freedoms in the post Covid-19 pandemic context.

29 <https://www.ohchr.org/en/instruments-listings>

30 <https://achpr.au.int/index.php/ar/node/3110>

31 <https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age#:~:text=In%20its%20resolution%20on%20the,in%20particular%20freedom%20of%20expression%E2%80%9D>

32 <https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr.pdf>

33 https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf

34 <https://www.osce.org/representative-on-freedom-of-media/78309>

35 <https://africaninternetrightrights.org/declaration/>

Table 1: Framework for conceptualising digital rights

Type of digital rights	Indicators
Access to information	Access to digital and social media platforms has become essential for the realisation of the free flow of information. Article 19 of the Universal Declaration of Human Rights explicitly upholds the freedom to seek, receive, and share information. The freedom to access information is meaningful only when internet content and applications are transmitted without undue discrimination or interference by non-state actors, including providers. Yet, restrictions on accessing digital and social media platforms through internet shutdowns, the blocking and filtering of content continue to become the norm in Africa.
Freedom of expression online	Freedom of expression is the right to express and receive opinions, ideas and information. Expression and exchanges of views increasingly take place online, including through social media platforms, websites and search engines. Yet, hate speech, and false news laws have been enacted with deleterious chilling effect.
Cybersecurity	It is about protecting internet-connected systems such as hardware, software and data from cyberthreats. These include cyber-fraud, hacking, phishing, ransomware, malware and DDOS attacks.
Right to privacy/ data privacy	Exercising privacy online is increasingly difficult in a world in which we leave a digital footprint with every action we take online. While data protection laws are on the rise in Southern Africa, they are of widely varying degrees of comprehensiveness and effectiveness, as well as enforcement. State-orchestrated mass surveillance is also on the rise as a result of the development of technology that enables the interception of communications in a variety of new ways, such as biometric data collection and facial recognition technology.

Source: Prof. Admire Mare

Social Context: A Brief Overview of Digital and Social Media in Southern Africa

The late 1990s were historical in the sense that they paved the way for the advent of the digital age in Southern Africa. Starting with the slow uptake of the internet, the region quickly embraced the mobile phone which replaced the ineffective landlines and postal services. The mobile phone allowed the region to leapfrog into higher stages of development in line with the modernisation theory. Besides allowing voice calls, the mobile phone came with short service messaging applications.

This opened up what has been termed the ‘parallel market of information’³⁶ in some authoritarian and monarchical regimes in Southern Africa. In these regimes, repressive and ideological state apparatuses are deployed to repress and suppress voices. The coming in of web 2.0 applications in the mid-2000s led to the mushrooming of various digital platforms. These included platforms like Myspace, Facebook, X (formerly Twitter), and YouTube. In South Africa, Mxit and Viber made significant inroads into the lives of mostly young people.³⁷

36 Moyo, D. (2009). Citizen Journalism And The Parallel Market Of Information In Zimbabwe's 2008 Election, *Journalism Studies*, 10:4, 551-567, DOI: 10.1080/14616700902797291

37 <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>



In the heart of Namibia, the #ShutItAllDown campaign emerged as a powerful testament to the transformative role of social media in activism, channeling voices from the streets of Windhoek to the global stage for justice and change. Photo: Vaultz.connect

This was followed by platforms such as Google+, Instagram, WhatsApp, and Pinterest. Besides the role played by web 2.0 technologies, it is noteworthy to emphasise that third generation (3G) of wireless mobile telecommunications technology significantly facilitated the adoption of relatively faster internet as opposed to the dial up service in Southern Africa.³⁸ The combination of web 2.0 applications and 3G technology led to a further reconfiguration of the digital ecosystem in the region. It unleashed an army of bloggers, social media users and vloggers with a huge appetite to share their own stories and narratives.³⁹ It is unsurprising that hashtag movements such as #FeesMustFall, #RhodesMustFall, #ShutItAllDown, #ZumaMustGo, #ZimbabweNationalShutdown, #ThisFlag and many others had a magnetic appeal amongst the youth and middle class because of the digital and social platforms.⁴⁰ These platforms have nurtured a unique environment for political discussions, cultural exchange, and economic transactions.⁴¹

Digital and social media platforms like Facebook, WhatsApp, Instagram, YouTube, X (formerly Twitter), and TikTok have provided an invaluable space for socialisation, communication, collaboration, and social interaction. These platforms have allowed Southern Africans to exercise 'digital citizenship'.⁴² However, the transition from analogue to digital forms of communication in Southern Africa was not a smooth ride.

Despite the fact that rates of internet and social media penetration are on the increase, there are structural factors that militate against universal access to digital technologies and their affordances. These include an underdeveloped telecommunications infrastructure, slow pace of rural and peri-urban electrification, high costs of data bundles and a general unwillingness amongst service providers to share telecommunication infrastructures.⁴³ Because of these deeply-embedded challenges, the region still suffers from digital divide and inequalities. These inequalities are also accentuated by power outages, which continue to punctuate the SADC region. For instance, in Zimbabwe, the Zimbabwe Electrical Supply Authority (ZESA), regularly implements power outages.⁴⁴

38 <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>

39 Somolu, O. (2007). Telling Our Own Stories': African Women Blogging for Social Change. *Gender and Development*, 15(3): 477-489.

40 Omanga, D., Mare, A. and Mainye, P. (2023). *Digital Technologies, Elections and Campaigns in Africa*. London: Routledge.

41 <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>

42 Ribble and Bailey (2007: 7) define digital citizenship as the ability of users to competently use digital technologies; interpret and understand digital content and assess its credibility; create, research, and communicate with appropriate tools

43 <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>

44 <https://www.news24.com/news24/africa/news/zimbabwe-is-back-to-20-hour-power-cuts-with-light-at-end-of-the-tunnel-only-in-2025-20231113>

Southern Africa had the highest internet penetration rate in Africa. Its internet penetration rate stood at 40.5 percent. This is in contrast with Eastern and Middle Africa which recorded 26 percent and 24 percent, respectively.

At least half of the population in Mozambique has no access to reliable electricity.⁴⁵ Statistics suggest that most Zambians have no access to electricity. The situation is equally bad in South Africa, which is the biggest economy in the region. The country has been experiencing loadshedding since 2007. The situation became dire just before the COVID-19 pandemic. Since then, loadshedding has become a daily ritual. This has had a knock on effect on access to the internet and social media technologies. Botswana and Namibia seem to faring better in terms of access to reliable electricity although they also buy some of their supply from South Africa and Zambia.

Statistics from the Internetworldstats⁴⁶ show that as of January 2022, Southern Africa had the highest internet penetration rate in Africa. Its internet penetration rate stood at 40.5 percent. This is in contrast with Eastern and Middle Africa which recorded 26 percent and 24 percent, respectively. With regards to national statistics on internet penetration, I present a summarised table below based on data from the Internetworldstats:

Figure 1: National statistics on internet penetration rates in some Southern Africa Development Community (SADC) countries

Country	Internet penetration rate (%)	Facebook subscribers 30 April 22
Angola	26%	2,875,600
Botswana	51.3%	1,191,300
Eswatini	56.4%	421,500
Lesotho	31.5%	553,900
Malawi	13.8%	637,600
Mozambique	20.3%	2,756,000
Namibia	52.1%	792,000
South Africa	57.5%	24,600,000
Zambia	52.2%	2,543,000
Zimbabwe	55.7%	1,303,000

Source: Internetworldstats⁴⁷, 2022.

It is important to underscore that the above statistics do not account for what has happened in the region between 2022 and 2024. For instance, the latest statistics from South Africa show that the internet penetration rate is at 74.7 percent.⁴⁸ Botswana has a penetration rate of 77.3% while Namibia’s rate is at 62.2%. It is noteworthy that most of the web traffic in Southern Africa emanates from mobile devices. This is not unique to Southern Africa. Similar conclusions have been reached by Global System for Mobile Association (GSMA)⁴⁹. Mobile internet access is the route through which most inhabitants of Southern Africa connect to the information superhighway. Relatively cheaper smartphones from the Asian market have enabled previously unconnected populations to have access to the internet. Social media bundles⁵⁰ have also enabled citizens to access the internet albeit without access to the full bouquet of the internet. Most citizens in Southern Africa have access to the internet through social media bundles, which are relatively cheaper packages when compared to uncapped broadband internet.

45 <https://www.sciencedirect.com/science/article/pii/S2214629621002164>

46 <https://www.internetworldstats.com/stats1.htm>

47 <https://www.internetworldstats.com/stats1.htm>

48 <https://datareportal.com/reports/digital-2024-south-africa>

49 <https://www.gsma.com/r/wp-content/uploads/2022/10/State-of-Mobile-Internet-Connectivity-2022-Sub-Saharan-Africa.pdf>

50 Data bundles are basically packages for internet access through a mobile device with a limit of bytes. The data bundles values change depending on the end-users payment: the more the users pay, the more bytes they get.

The enactment of data protection legislation and policy, the development of jurisprudence on digital rights, and increased advocacy from civil society actors on digital rights, are some of the major wins in the last five years.

They have played an instrumental role in allowing lower and middle classes to have access to some kind of internet. However, this has been critiqued for violating net neutrality principles by digital rights activists. Critics argue that zero-rating prioritises certain services over others, and therefore challenges the net neutrality principle while harming market competition and innovation.⁵¹

Methodological Approach

This study was anchored in qualitative research methodology. This methodology is used to answer questions about experiences, meanings and perspectives from the standpoint of the participants.⁵² The report is based on primary and secondary data drawn from qualitative policy analysis and document analysis as well as interviews with key informants from a selected pool of SADC countries. Key informants were relevant for the purposes of understanding the current state of digital rights in the region from the perspective of situated actors. Qualitative policy analysis and document analysis entail an analysis of texts and documents, such as civil society reports, media articles, laws and regulations, policy briefs and websites. Qualitative policy analysis was used to make sense of existing legislation, policies, and regulations enabling or infringing the exercise of digital rights in Southern Africa. It included a comprehensive desktop review of international, regional, and domestic digital rights literature, inclusive of legal and policy documents, research reports, and other scholarly resources. Ten in-depth interviews were conducted with key informants drawn from Namibia, Mozambique, Malawi, South Africa, Zambia and Zimbabwe to get insider perspectives on the state of digital rights with regards to cybersecurity, digital privacy, access to information and freedom of expression online.

Most of these interviewees were media and data rights activists, academics, journalists and human rights defenders. Interviews were also important for verifying the accuracy and authenticity of existing literature. Informed consent was sought, and anonymity was guaranteed due to the sensitive nature of the research.

Key Findings

It is poignant to note that there are a number of positives that have been registered in the area of digital rights over the last few years. The enactment of data protection legislation and policy, the development of jurisprudence on digital rights, and increased advocacy from civil society actors on digital rights,⁵³ are some of the major wins in the last five years. For instance, countries such as South Africa, Zambia and Zimbabwe have access to information laws in their statute books. The Zambian parliament adopted the access to information legislation in December 2023.⁵⁴ The Act goes a long way in providing a strong foundation for the enjoyment of the right to information as provided for in the African Charter and Zambia's Constitution.⁵⁵ In recent years, countries such as Zambia and Zimbabwe passed the Data Protection Act, No. 3 of 2021⁵⁶ and Cyber and Data Protection Act of 2021⁵⁷ respectively.

51 <https://dig.watch/topics/network-neutrality#:~:text=Opponents%20argue%20that%20zero%2Drating,harming%20market%20competition%20and%20innovation>

52 Hammarberg, K, Kirkman, M and de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. Human Reproduction, 31(3): 498-501.

53 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

54 <https://ipi.media/zambia-ipi-welcomes-enactment-of-the-access-to-information-law/>

55 <https://ipi.media/zambia-ipi-welcomes-enactment-of-the-access-to-information-law/>

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

57 <https://www.veritaszim.net/node/5522#:~:text=This%20Act%20may%20be%20cited,%5BChapter%2012%3A07%5D.&text=The%20object%20of%20this%20Act,their%20representatives%20and%20data%20subjects>



Empowering African women entrepreneurs, internet access and mobile technology have become pivotal tools, transforming traditional markets into vibrant digital arenas for online transactions and business innovation. Photo: Freepik

In the Zambian context, the Data Act provides a framework for how personal data can be used and protected.⁵⁸ It also regulates how personal data should be collected, used, transmitted, stored and processed, among other functions. The country ratified the 2014 African Union's Malabo Convention on Cyber Security and Personal Data Protection.⁵⁹ Other SADC countries which have ratified the Convention include Angola, Mozambique, Mauritius, and Namibia.⁶⁰ The Zambian government also enacted the Cyber Security and Cyber Crimes Act and the Electronic Communications and Transactions Act on the day the Data Protection Act was assented.

Eswatini enacted the Computer Crime and Cyber Crime Act, 2022, the Data Protection Act, 2022, and the Electronic Communications and Transactions Act, 2022.⁶¹ In the case of Botswana, the Data Protection Act was meant to come into force when the grace period ended on the 15th of October 2022, but it has since been extended for another year.⁶² The delays in implementing the law has been necessitated by the glaring gaps identified in the 2021 version of the Act. It was realised that the legislation does not cover the processing of personal data in the course of a purely personal or household activity and lacks detail regarding the processing of data for national security, defence or public safety including for the prevention of and investigation into offences.⁶³ South Africa has the Promotion of Equality and Prevention of Unfair Discrimination Act, 2000 (the Equality Act) aimed at preventing hate speech. The Act allows for both civil and criminal remedies against hate speech and other harmful speech, both offline and online.⁶⁴ Namibia is also in the process of finalising its data protection law after several false starts.⁶⁵ The draft data protection bill seeks to govern the processing of personal data conducted within and outside the country.⁶⁶

And is aligned with SADC model laws on cybercrime, electronic transfers and personal data protection.

Despite these great strides, digital rights violations have also been flagged in some Southern African countries. One major concern has increasing cases of insidious forms of unlawful surveillance⁶⁷ in Angola, DRC, Eswatini, Lesotho, Malawi, Mozambique, Namibia, Zambia and Zimbabwe.⁶⁸ Most of these practices have taken the form of mobile phone tapping, social media monitoring, facial recognition systems, safe city projects, cloud computing infrastructures, and smart policing initiatives.⁶⁹

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

59 <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

60 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

61 <https://www.apc.org/en/news/eswatini-passes-cyber-laws-under-dark-clouds>

62 <https://www.michalsons.com/blog/botswanas-data-protection-act-grace-period-extended/60775>

63 <https://itweb.africa/content/LPp6V7rB1Kg7DKQz>

64 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

65 <https://www.namibian.com.na/information-deputy-minister-underscores-importance-of-personal-data-protection/>

66 <https://www.namibian.com.na/information-deputy-minister-underscores-importance-of-personal-data-protection/>

67 Munoriyarwa, A. And Mare, A. (2022). *Digital Surveillance in Southern Africa: Policies, Politics and Practices*, Cham: Springer.

68 <https://cipesa.org/2023/09/sifa2023/>

69 https://researchictafrica.net/wp/wp-content/uploads/2021/01/AI-Surveillance_Policy-Brief_Oarabile_Final.pdf

Over and above the unlawful digital surveillance practices, concerns have been raised around the use of Strategic Litigation Against Public Participation (SLAPP) suits and network throttling during elections and protests.

A case in point is the lack of transparency and accountability around the smart cities project in Zambia,⁷⁰ which is particularly harmful in the absence of adequate oversight mechanisms. The smart city initiative has been established without necessary and proportionate safeguards that protect human rights against encroaching surveillance practices.⁷¹ Reports also suggest that Zimbabwe is on course to establish its own cyber city project. As if that is not enough, artificial intelligence-driven surveillance technologies are also being deployed in Zimbabwe. Security agencies have also installed closed-circuit television (CCTV) cameras in Harare and Bulawayo with a focus on major streets and Africa Unity Square across from the National Assembly building — all locations popular with anti-government protesters.⁷² This represents a calculated assault on citizens' constitutional right to privacy.

Over and above the unlawful digital surveillance practices, concerns have been raised around the use of Strategic Litigation Against Public Participation (SLAPP) suits and network throttling during elections and protests.⁷³ Interviews with key informants in the SADC region revealed that poor governance over personal data, privacy rights breaches, limitations on the freedom of expression, assembly and association online, online-gender-based violence against journalists⁷⁴ and women in politics⁷⁵ and criminalisation of online speech are some of the teething challenges facing the region. Other challenges related to digital rights include the gender digital divide, online harassment and violence particularly against women and girls. In the sections that follow, this report focuses on the current state of digital rights with regards to the four pillars discussed earlier. These are the freedom of expression online, access to information, cybersecurity and data privacy.

a) Freedom of expression online

The right to freedom of expression includes the freedom to hold opinions without interference and to seek, receive and impart information.⁷⁶ As articulated earlier, it is well protected by domestic, regional and international human rights frameworks. In the African context, freedom of expression is protected under article 9 of the African Charter, which confers the right to receive information, and the right for every individual to express and disseminate their opinion within the scope of the law.⁷⁷ Suffice to say that the right to freedom of expression is not absolute and may be limited in certain circumstances. Although most countries have well-developed bills of rights in their constitutions, violations of freedom of expression online have been documented. These undue restrictions on the right to freedom of opinion and expression online undermine democracy and the rule of law. Southern African states have adopted new cybercrime laws that criminalise the communication of false information on social media and the Internet.^{78 79} In most cases, some of these laws duplicate existing criminal and penal code sanctions for defamation.⁸⁰

70 https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/zambia_report.pdf

71 https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/zambia_report.pdf

72 <https://adf-magazine.com/2023/01/zimbabwe-turns-to-chinese-technology-to-expand-surveillance-of-citizens/>

73 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

74 <https://journals.sagepub.com/doi/10.1177/01968599231210790>

75 <https://journals.sagepub.com/doi/full/10.1177/14648849231183815>

76 <https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2019,media%20and%20regardless%20of%20frontiers>

77 https://www.justice.gov.za/policy/african%20charter/1981_AFRICAN%20CHARTER%20ON%20HUMAN%20AND%20PEOPLES%20RIGHTS.pdf

78 <https://namibiafactcheck.org.na/news-item/sadc-states-already-have-problematic-measures-to-deal-with-fake-news/>

79 Salau, A. O. (2020). 'Social media and the prohibition of 'false news': can the free speech jurisprudence of the African Commission on Human and Peoples' Rights provide a litmus test?' (2020) 4 *African Human Rights Yearbook* 231-254. <http://doi.org/10.29053/2523-1367/2020/v4a12>

80 <https://www.ahry.up.ac.za/salau-ao>

At the height of the COVID-19 pandemic, a number of countries (including Namibia, South Africa, Zimbabwe) managed to sneak in laws that prohibited the spread of fake news.⁸¹ South Africa introduced them after a flood of COVID-related fake information and photographs were spread on WhatsApp, SMS, and email – causing significant panic and anxiety for the general public.⁸² In some countries, governments have responded to the growing disinformation trends by weaponising disinformation laws to stifle legitimate expression while hampering access to critical and pluralistic information.⁸³ Content-regulation measures, such as the law passed in Angola in 2017 which established a Social Communication Regulatory Body that is empowered to investigate online content producers and suspend websites that are deemed not to meet good standards of journalism, is a cause for concern. These laws have been abused to significantly curtail freedom of expression online in some jurisdictions.

A close reading of Zimbabwe’s Cyber and Data Protection Act suggests a subtle strategy to securitise the online space and further erode the Bill of Rights as enshrined in the 2013 Constitution. The criminalisation of the spread of false news and narratives is a case in point. Under clause 164C of the Act, the government criminalises what it classifies as the transmission of “false information” that incites violence or damage to property. Concepts such as ‘false information’ and ‘incite’ have not been lucidly defined thereby opening up room for abuse. Incitement laws in Zimbabwe have in the past been used to target digital activists. The danger is that clause 164C could be used to silence those who use online platforms to expose corruption - often within government institutions - a key purpose of journalism. Since August 2022, at least three Zimbabwean journalists have been arrested under the Data Protection Act. They are Wisdom Mdzungairi (the former editor-in-chief for Alpha Media Holdings and editor of *NewsDay* newspaper), Desmond Chingarande (a senior reporter at *NewsDay*, and Hope Chizuzu (freelance sports journalist).⁸⁴ Wisdom and Desmond were arrested in August 2022 on charges of transmitting “false data intending to cause harm.”⁸⁵

The offense carries a fine of 70,000 Zimbabwean dollars (US\$193) and up to five years in prison. In September 2022, sports freelance journalist, Hope Chizuzu, was also arrested.⁸⁶ This was after Moses Chunga and Eric Aisam, Dynamos Football Club board members, opened a case against him for allegedly transmitting false messages. Chizuzu, who mostly publishes stories on Facebook, was charged with transmitting false data messages intending to cause harm, in violation of Section 164C of the Data Protection Act.⁸⁷ The police officers also confiscated his mobile phone and an iPad.⁸⁸ This was a clear case where the law was abused by people accused of corruption to silence a whistleblower. Aside from journalists - human rights defenders, content creators and political activists, have also been arraigned before courts of law. A Zimbabwean TikToker, David Kanduna, was the first person to be convicted under the Data Protection Act.⁸⁹ This was after Kanduna recorded a video of a police officer being hoisted and jeered during skirmishes at Chinhoyi University of Technology.⁹⁰ He was convicted of cyberbullying a police officer under section 164B of the Data Protection Act. He was given the option of paying a fine of ZWL3,000 or going to jail for 20 days.⁹¹

81 <https://www.namibian.com.na/covid-19-fake-news-now-a-crime/>

82 <https://csirt.uct.ac.za/awareness-cybersecurity-month-cybersecurity-month-2020/south-africa-brings-law-place-stop-spread-fake-covid-19-news>

83 https://cipesa.org/wp-content/files/reports/SIFA23_Report.pdf

84 <https://cpj.org/2022/08/zimbabwe-police-charge-2-journalists-with-publishing-false-information/>

85 <https://cpj.org/2022/08/zimbabwe-police-charge-2-journalists-with-publishing-false-information/>

86 https://zimbabwe.misa.org/media_violations/journalist-arrested-and-charged-for-publishing-falsehoods/

87 https://zimbabwe.misa.org/media_violations/journalist-arrested-and-charged-for-publishing-falsehoods/

88 https://zimbabwe.misa.org/media_violations/journalist-arrested-and-charged-for-publishing-falsehoods/

89 [https://www.newzimbabwe.com/tik-toker-fined-zw3-000-for-cyberbullying-police-officer/#:~:text=David%20Kanduna%20\(23\)%2C%20who,but%20controversial%20Data%20Protection%20Act](https://www.newzimbabwe.com/tik-toker-fined-zw3-000-for-cyberbullying-police-officer/#:~:text=David%20Kanduna%20(23)%2C%20who,but%20controversial%20Data%20Protection%20Act)

90 [https://www.newzimbabwe.com/tik-toker-fined-zw3-000-for-cyberbullying-police-officer/#:~:text=David%20Kanduna%20\(23\)%2C%20who,but%20controversial%20Data%20Protection%20Act](https://www.newzimbabwe.com/tik-toker-fined-zw3-000-for-cyberbullying-police-officer/#:~:text=David%20Kanduna%20(23)%2C%20who,but%20controversial%20Data%20Protection%20Act)

91 [https://www.newzimbabwe.com/tik-toker-fined-zw3-000-for-cyberbullying-police-officer/#:~:text=David%20Kanduna%20\(23\)%2C%20who,but%20controversial%20Data%20Protection%20Act](https://www.newzimbabwe.com/tik-toker-fined-zw3-000-for-cyberbullying-police-officer/#:~:text=David%20Kanduna%20(23)%2C%20who,but%20controversial%20Data%20Protection%20Act)

These cases demonstrate that freedom of expression is under threat in the context of the Data Protection Act, which has been weaponized by the ruling elite.

In Angola, a popular social media influencer, Ana da Silva Miguel, known as Neth Nahara, was imprisoned for "insulting" President João Lourenço on TikTok in October 2023.⁹² On 10 February 2024, Joaquim Pachoneia, also known as Jota, was arrested in Mozambique for producing and distributing videos on WhatsApp inciting citizens in Nampula to act violently against state institutions.⁹³ In 2020, Tanzania introduced the Online Content Regulation aimed at regulating hate speech.⁹⁴ The country graced international headlines when it announced plans to introduce systems to regulate the publication of online content outside of public communications.⁹⁵ These regulations have been criticised for lacking clarity and conferring discretionary powers to service providers to determine what constitutes criminal activity, and the role of banning content that uses 'bad language'.⁹⁶ In June 2022, in an attempt to curb the spread of disinformation on terrorism and conflict in the Carbo Delgado region, the Mozambican government introduced the Law for Suppression, Combat, and Prevention of Terrorism and Related Actions.⁹⁷ Article 19(1) of the Act stipulates that "whoever, by any means, discloses information classified under this Law, shall be punished with imprisonment from 12–16 years." Clearly, such a provision has the collateral consequence of criminalising journalism as well as citizens in general, and not those who have the duty to safeguard "State Secrets" in this case, public servants or officials holding such classified information.⁹⁸ It also has a specific clause which states that whoever intentionally disseminates information on the occurrence or otherwise of a terrorist attack, knowing that the information is false, will be punished with imprisonment between 8 to 12 years.⁹⁹

Freedom of expression online is also being stifled by the high cost of data. In most countries, the internet is priced beyond the reach of the majority of the citizens. Average data costs in Zimbabwe are higher than in neighbouring countries, far exceeding the average of \$1.81 for 1GB in South Africa, \$0.38 in Malawi or \$0.78 in Mozambique and \$1.26 in Eswatini.¹⁰⁰ In Malawi, for example, a monthly data bundle of 10GB costs MK15, 500 (\$20) at TNM and Airtel.¹⁰¹

This is approximately half the monthly income of the average Malawian. The minimum wage stands at K35, 000 (\$47). In a way, high prices are being weaponised to curtail the enjoyment of freedom of expression online. Censorship through internet shutdowns and network disruptions in Democratic Republic of Congo, Eswatini, Tanzania, Zambia and Zimbabwe have also further contributed to digital rights violations. More than any other SADC country, Zimbabwe has implemented several internet shutdowns in recent years, particularly during periods of political and social upheaval. In 2016, during the #MugabeMustFall and #ThisFlag campaigns, social media platforms were temporarily switched off. In 2019, following a challenge by human rights groups to a directive issued by the Minister of State for an internet shutdown, the High Court ruled that the directive was unlawful. Despite the 2019 High Court ruling, on 30 July and 1 August 2020, Zimbabwe experienced further internet shutdowns at the same time as the #July 31 protests. The state-owned network provider, TelOne, has been reported to have throttled connectivity speeds. In the run up to the August 2023 elections, digital and social media platforms were throttled.

Content moderation practices by internet intermediaries and platforms companies have also significantly affected the enjoyment of freedom of expression online. Content moderation is the process of reviewing and monitoring user-generated content on online platforms to ensure that it meets certain standards and guidelines.¹⁰²

96 <https://www.article19.org/resources/tanzania-online-content-regulations-problematic-covid-19-pandemic/>

97 <https://jamlab.africa/mozambiques-new-laws-undermine-freedom-of-expression-and-press/>

98 <https://www.voanews.com/a/mozambique-approves-tough-anti-terror-bill-/6582319.html>

99 <https://jamlab.africa/mozambiques-new-laws-undermine-freedom-of-expression-and-press/>

100 <https://www.cable.co.uk/mobiles/worldwide-data-pricing/>

101 https://www.upinfo.org/sites/default/files/documents/202010/5._centre_for_human_rights_and_rehabilitation_stmt.pdf

102 <https://besedo.com/knowledge-hub/blog/what-is-content-moderation/>



The unchecked expansion of surveillance technology in Africa is altering the governance framework, potentially serving as a new instrument of oppression. Photo: ISS

The negative effects of untargeted or disproportionate content moderation have been shown to disproportionately impact marginalised persons, mainly through disregarding their experiences on digital and social media.

More often than not, it often results in the removal or down-ranking of certain information from a digital platform, either in line with a platform’s own policies or guidelines or as the result of national laws or regulations.¹⁰³ The opaque enforcement of community guidelines and standards by platform companies has been criticised for being inconsistent, non-transparent, and in some instances, harmful.¹⁰⁴ The negative effects of untargeted or disproportionate content moderation have been shown to disproportionately impact marginalised persons, mainly through disregarding their experiences on digital and social media.

b) Privacy and data protection

As discussed earlier, most countries in South Africa have passed data protection laws aimed at promoting and protecting the right to privacy. This is important given the extensive data mining and extraction of data for business without consideration for impacts on human rights.¹⁰⁵ For example, South Africa has been a torch bearer in the promulgation of data protection laws. Whereas other countries started working on their draft bills in 2020, South Africa passed the Protection of Personal Information Act in 2013.¹⁰⁶ The law adopted an extraterritorial approach, which means that entities outside of the country that handle citizens’ data are subject to the law.¹⁰⁷

103 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

104 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf

105 <https://www.oru.se/contentassets/981966a3fa6346a8a06b0175b544e494/zuboff-2019.pdf>

106 [https://popia.co.za/#:-:text=Parliament%20assented%20to%20POPIA%20on,110%20and%20114\(4\).](https://popia.co.za/#:-:text=Parliament%20assented%20to%20POPIA%20on,110%20and%20114(4).)

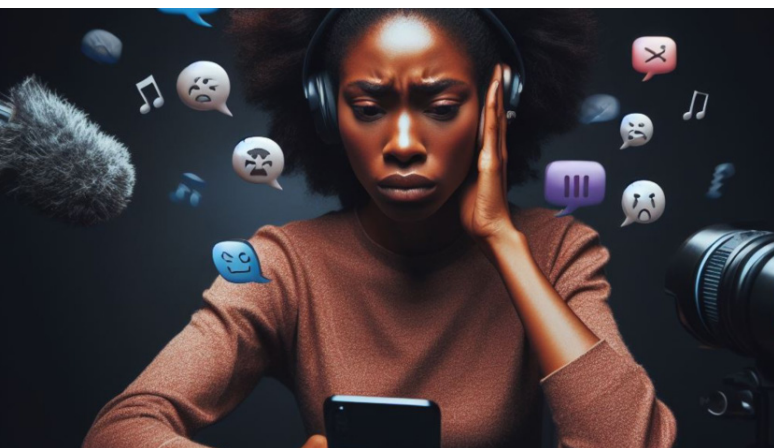
107 [https://popia.co.za/#:-:text=Parliament%20assented%20to%20POPIA%20on,110%20and%20114\(4\).](https://popia.co.za/#:-:text=Parliament%20assented%20to%20POPIA%20on,110%20and%20114(4).)

Article 17 of the Zambian Data Protection Act of 2021, for instance, provides for the right to privacy including the right not to be searched (person, home or property); not to have possessions seized; not to have information relating to family, health status and private affairs unlawfully required or revealed; and not to have communications infringed.¹⁰⁸ Notwithstanding these progressive provisions, some of the data protection laws in the region are selectively enforced. At a continental level, there is still no harmonised mechanism being consistently implemented to support human-rights-centric cross-border data flows. This puts Southern African states at risk of exporting their data outside the continent without necessary protections.

Violations around the right to privacy and data protection have been heightened by the indiscriminate use of digital technologies for surveillance purposes.¹⁰⁹ In the SADC region, countries such as Angola, Botswana, Mauritius, Namibia, South Africa, Zambia, and Zimbabwe have been singled out in the AI Global Surveillance (AIGS) Index produced by the Carnegie Endowment for International Peace for using AI and big data surveillance tools (including smart city sensors, facial recognition, and smart policing).¹¹⁰ Although the Index does not differentiate between legitimate and illegitimate use of AI tools for surveillance by these countries, it provides a snapshot of the state of affairs.

The growing uptake of digital technologies has led to calls for adequate legal frameworks to ensure the protection of privacy and personal data. Interviews with key informants in Namibia and South Africa have shown that communication surveillance often takes place outside of the legal framework. Mobile phone interception technologies are also popular among Southern African governments. These technologies are generally used for covert spying on citizens' phone calls, text messages, instant messaging or internet communications using a mobile phone.

Only 8 of 12 SADC countries surveyed (Angola, Botswana, Democratic Republic of Congo, Eswatini, Lesotho, South Africa, Namibia, and Zambia) have provisions for a legal requirement for a judge or court to authorise the interception of communications, which is considered a basic oversight feature of interception laws. With the exception of Angola and South Africa, most laws in the region do not address the issue of proportionality. Some Southern African countries have enacted mandatory SIM card registration laws which in essence create a surveillance target database. For instance, the Namibian Communications Act of 2009 requires telecommunications operators to collect basic information such as names, dates of birth, addresses, and copies of identification documents to register a SIM card. This requirement has been vigorously enforced since June 2022.¹¹¹ The government reported that as of the end of 2023, 62.5 percent of active SIM card users had registered.¹¹² This translates to 1.49 million registered people out of a total population of 2.38 million. The registration deadline has been extended from 31 December 2023 to 31 March 2024.¹¹³



Women journalists confront a relentless tide of online violence, a stark reminder of the challenges that persist in silencing their crucial narratives. Source for pic: African Centre for Media Excellence (ACME)

108 <https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf>

109 Munoriyarwa, A. And Mare, A. (2022). *Digital Surveillance in Southern Africa: Policies, Politics and Practices*, Cham: Springer.

110 <https://carnegieendowment.org/publications/interactive/ai-surveillance>

111 <https://www.namibian.com.na/govt-extends-sim-card-registration-deadline-to-march/>

112 <https://itweb.africa/content/xnklOqz1jWWM4Ymz>

113 <https://itweb.africa/content/xnklOqz1jWWM4Ymz>

The increasing cases of interception of communication and surveillance in Southern Africa have led to wanton violations of citizens' right to privacy.

Countries such as Botswana, the Democratic Republic of Congo, Eswaini, Kenya, Tanzania, Uganda, Zambia and Zimbabwe have also enacted SIM card registration laws.¹¹⁴ The increasing cases of interception of communication and surveillance in Southern Africa have led to wanton violations of citizens' right to privacy. It has also affected the enjoyment of several human rights and freedoms as enshrined in national, regional, and international instruments. It poses enormous threats to the realisation and enjoyment of digital rights. It affects the ability of individuals and organisations to organise, mobilise, and engage in democratic processes. It contributes to the curtailment of rights to freedom of expression, access to information, association and assembly. It nurtures an uncomfortable climate of chilling effects, which leads to self-censorship, political resignation, and apathy.

c) Access to information

Access to information laws are critical as they enable investigative journalists and citizens alike to request information from public institutions, which are obliged to provide such information within reasonable timelines. Most of the SADC countries have made domestic and international commitments to take steps towards achieving universal access to online information. This has been captured in the recently passed laws. For instance, Zambia passed its Access to Information Act in 2023.¹¹⁵ It seeks to provide for the right to access information and its limitations; provide for procedures for processing requests for information; and give effect to the right to access information as guaranteed in the United Nations Convention against Corruption and the African Charter on Human and Peoples Rights.¹¹⁶

South Africa introduced the Promotion of Access to Information Act in 2000, which aimed to "actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights."¹¹⁷ Zimbabwe introduced the Freedom of Information Act in 2020,¹¹⁸ which replaced the egregious Access to Information and Protection of Privacy Act of 2001.¹¹⁹ In Namibia, the Access to Information Act 8 of 2022 was passed by parliament and signed by the president on 29 November 2022.¹²⁰ However, it has not yet been brought into force. Despite the passage of the laws, access to information online is still hampered by limited access to the internet. The cost of acquiring hardware and software also militates against the enjoyment of access to information online. In countries like South Africa, plans are afoot in some to provide universal and free internet access. This includes the gradual introduction of free municipal Wi-Fi as a basic service and access at other government sites, and rolling out digital literacy programmes. There is urgent need to ensure all the countries align the laws with the African Model Law on Access to Information, published by the African Commission on Human and Peoples' Rights in 2013.

114 Hunter, M. and Mare, A. (2020). Patchwork For Privacy: Communication Surveillance In Southern Africa. MPDP: Johannesburg.

115 <https://www.parliament.gov.zm/node/11547>

116 <https://www.parliament.gov.zm/node/11547>

117 <https://www.gov.za/documents/promotion-access-information-act>

118 <https://www.veritaszim.net/node/4282>

119 <https://www.veritaszim.net/node/240#:~:text=An%20Act%20to%20provide%20members,or%20disclosure%20m of%20personal%20information>

120 <https://www.lac.org.na/laws/2022/7986.pdf>

d) Cybersecurity

Taking cue from the Malabo Convention on Cyber Security and Personal Data Protection, a handful of Southern African countries have passed standalone laws on cybersecurity.¹²¹ The Convention places a positive obligation on Member States to adopt the necessary domestic measures to safeguard personal information, including by enacting legal frameworks for data protection and establishing National Data Protection Authorities.¹²² The Convention has been criticised for criminalising “insulting language.”¹²³ Although the development of cybersecurity and data protection laws in Southern Africa lagged behind many parts of the continent, the region has made significant progress in recent years, particularly since 2020. In 2022, President Hakainde Hichilema, agreed to review Zambia’s controversial Cyber Security and Cyber Crime enacted in 2021. It was meant to combat cybercrime, coordinate cyber security matters, develop relevant skills and help promote the responsible use of social media in addition to facilitating the identification, declaration and protection of national critical infrastructure.¹²⁴ Countries such as Zimbabwe introduced an omnibus law which deals with electronic transactions, cybercrimes and data protection in 2021. A major concern has been long delays in implementation, which is partly due to the poor resourcing and operationalisation of Data Protection Authorities (DPAs). For example, while Angola’s data protection law, Laws No. 22/11, was signed into law in 2011, the enforcement authority was not established until 2019.¹²⁵ South Africa’s data protection law, the Protection of Personal Information Act (POPIA), was signed into law in 2013.¹²⁶ Its different provisions came into force incrementally until the entire Act came into effect in July 2021.¹²⁷ The Democratic Republic of Congo adopted a Digital Code which includes provisions relating to data protection.¹²⁸ The Code establishes new regulators and contains provisions on data collection, processing, transfer and storage; e-signatures; advertising and marketing; consumer protection; electronic evidence; data interception; subcontractors; and benefits for digital start-ups.¹²⁹

Cybercrimes have also become more pronounced in online spaces, often targeting women, girls, and gender and sexual minorities.¹³⁰ Women in politics have also been on the receiving end of hate speech, sexualised commentary and name calling.¹³¹

This has been confirmed by the report on trends and policy frameworks relating to Online Gender-Based Violence (OGBV) in Angola, Botswana, Malawi, Mozambique, Namibia, South Africa, Zambia, and Zimbabwe.¹³² In February 2024, there were media reports that Zimbabwean businessman and socialite, Wicknell Chivayo, threatened young female journalist Rutendo Maraire who attempted to get a comment for the article she was working on.¹³³ The situation on OGBV has been exacerbated by the fact that there are insufficient legal protections and inadequate government actions.

In the aftermath of Al Jazeera’s 2023 Gold Mafia documentary, journalists, including Hopewell Chin’ono in Zimbabwe, have been particularly targeted, prompting them to cease reporting on developments related to the documentary as a measure to protect their safety. And in terms of data privacy violations, in the run up to August 2023 elections, the Zimbabwe Electoral Commission (ZEC) reported that it had recorded over a hundred failed attempts to hack into its voters roll server.¹³⁴

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

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

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

124 <https://itweb.africa/content/GxwQD71DVkYvIPVo>

125 <https://dataprotection.africa/angola/#:~:text=While%20the%20law%20was%20signed,no%20significant%20level%20of%20enforcement>

126 [https://popia.co.za/#:~:text=The%20commencement%20date%20of%20POPIA&text=Parliament%20assented%20to%20POPIA%20on,110%20and%20114\(4\)](https://popia.co.za/#:~:text=The%20commencement%20date%20of%20POPIA&text=Parliament%20assented%20to%20POPIA%20on,110%20and%20114(4))

127 <https://www.simplepay.co.za/popia#:~:text=Since%20its%20passing%20into%20law,commenced%20on%201%20July%202020>

128 <https://ecomafrika.org/blog/2023/06/05/democratic-republic-of-congo-drc-has-adopted-a-digital-code/>

129 <https://ecomafrika.org/blog/2023/06/05/democratic-republic-of-congo-drc-has-adopted-a-digital-code/>

130 <https://www.oas.org/en/sms/cicte/docs/Guide-basic-concepts-Online-gender-based-violence-against-women-and-girls.pdf>

131 <https://www.taylorfrancis.com/chapters/edit/10.4324/9781003429081-3/twitter-elections-gendered-disinformation-campaigns-zimbabwe-admire-mare>

132 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/FINAL_v_Understanding_oGBV_in_Southern_Africa.pdf

133 <https://businesstimes.co.zw/sir-wicknel-attack-on-female-journo-sparks-outrage/>

134 <https://www.newzimbabwe.com/zec-reveals-there-have-been-over-a-hundred-attempts-to-hack-into-voters-roll-server-but-disputes-allegations-team-pachedu-has-a-copy/>

A Call to Action

Practical Advocacy Interventions

In order to push back against digital rights and freedom violations, this report proposes the following policy advocacy interventions aimed at stakeholders such as civil society, policymakers, NGOs, and the general public. These interventions are also targeted at the Special Rapporteur on Freedom of Expression and Access to Information in Africa of the African Commission for Human and Peoples' Rights (ACHPR). The report makes the following practical advocacy interventions:

- Governments should repeal, amend, or review existing laws, policies, and practices on cybersecurity, data protection, access to information, and interception of communication and surveillance to ensure compliance with regional and international human rights standards.
- Governments should repeal all claw back clauses on cybersecurity, data protection, access to information, and interception of communication and surveillance in line with the requirements of the UN Special Rapporteur on Freedom of Expression and Access to Information in Africa of the African Commission for Human and Peoples' Rights.
- Governments should ensure that universal service and access funds (USAFs) collected from telecommunication operators are used to fund projects and programmes that strive to achieve universal service and access to ICTs by all citizens in Southern Africa.
- Governments should ensure the provision of affordable and reliable electricity in order to promote access to regular and affordable internet and social media services.
- Judiciaries, Parliaments and Data Protection Authorities should provide comprehensive and independent oversight over the state and its agencies in their surveillance operations.
- The media should investigate, document and publish stories highlighting the risks presented by communication interception and surveillance to human rights.
- The media should spotlight suppliers, customers, and the users of surveillance technologies.
- Academia should conduct evidence-based research on cybersecurity, data protection, disinformation, internet shutdowns, and communication interception and surveillance and its human rights impact.
- Academics should partner with civil society organisations in collecting evidence-based information and advocacy on disinformation, data protection, access to information online, and interception of communication and surveillance in Southern Africa.
- Civil society organisations (CSOs) should investigate, document, and expose human rights violations arising from internet shutdowns, SIM card registration requirements, and communication interception and surveillance.
- CSOs should engage in strategic public interest litigation to challenge internet shutdowns, disinformation, online gender-based violence, and surveillance laws, measures and practices.
- CSOs should enhance their cybersecurity and data protection measures. Intermediaries should regularly publish, update, and widely disseminate privacy policies and transparency reports regarding content moderation and surveillance.
- Intermediaries should put in place privacy and data protection policies and inform users about the measures taken to protect their right to privacy.
- Vendors of surveillance technologies should conduct human-rights assessments and inculcate due diligence measures in compliance with the UN Guiding Principles on Business and Human Rights.

Conclusion

This report has shed light on the extent to which SADC countries are complying with regional, international and national legislation requiring them to promote and protect the right to freedom of expression, access to information, right to privacy and cybersecurity in the digital age. Drawing on key informant interviews and desktop research, the report has highlighted some of the positive developments associated with the passage of progressive data protection laws, setting up of data protection authorities, promotion of free expression online, amendment of access to information laws and promotion of the safety of journalists online. It has also discussed negative developments as evidenced by the introduction of claw back clauses around the publication and distribution of false news, passage of draconian cybercrime laws, digital surveillance practices, internet shutdowns and throttling, harassment and intimidation of journalists online, introduction of mandatory SIM Card registrations, and imprisonment of citizens and human rights defenders for online speech. It proffers advocacy interventions that civil society groups in the region including the NMT, MISA Regional, Spaces of Solidarity, CIPESA, PI and the CHR can implement to protect the realisation of digital rights in the region. Overall, the report recommends that collective effort, from various stakeholders, including governments, intermediaries, civil society, the media, and academia, is needed in order to promote right to freedom of expression, access to information, right to privacy and cybersecurity in the digital age.



About the Author: Admire Mare is an Associate Professor and Head of Department: Communication and Media Studies, University of Johannesburg, South Africa with an interest in digital rights, technology, platform justice, digital journalism, platformisation of everyday life and the nexus between data and society. He is the Thought Leader in Chief at Denhe Re-ruzivo Consultancy Hub.